Dell EMC OpenManage Network Manager Version 6.5

User Guide



Notes and Cautions

A NOTE indicates important information that helps you make better use of your computer.

A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

© 2017 Dell Inc.

Trademarks used in this text: Dell EMC™, the DELL EMC logo, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, KACE™, FlexAddress™ and Vostro™ are trademarks of Dell Inc. Microsoft®, Windows®, Windows Server®, MS-DOS® and Windows Vista® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat Enterprise Linux® and Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries.

Other trademarks and trade names may be used in this publication to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

2017-9

Rev. A01

Contents

Preface

Why OpenManage Network Manager? . . . 15
Application Overview . . . 16
Key Features . . . 17
Networks with Dell EMC OpenManage Network Manager . . . 17
Additional Products . . . 18
Online Help/Filter . . . 19
A Note About Performance . . . 20
Guide Revision Record . . . 21

1 Getting Started . . . 23

General Information . . . 24
Web Portal/Multitasking . . . 24
Cookies and Sessions . . . 24
Web Clients . . . 24
Network Basics . . . 25
Starting/Stopping OMNM . . . 27
Starting/Stopping Servers . . . 27
Starting Web Client . . . 28
Setting Up Secure Connections (SSL & HTTPS) . . . 28
Enabling Secure SSL . . . 29
Turning on SSL Within the Web Portal . . . 30
Managing Users and Permissions . . . 31
Adding Users and Connecting them to Roles . . . 32
Adding and Configuring User Roles/Permissions . . . 34
Adding Individual Permissions . . . 36
Adding LDAP Users . . . 36
Creating an LDAP Admin User . . . 37
Implementing DAP . . . 38
Opening an Archive in dapviewer . . . 39
Backing Up the Database . . . 39
Restoring Databases . . . 40
Setting Up Authentication . . . 41
Integrating LDAP . . . 41
Configuring a CAS Server with RADIUS . . . 44
Setting Up Radius Authentication . . . 47
Configuring Pages and User Access . . . 48
Creating Users . . . 49
Creating and Rearranging Pages . . . 49
Setting Page-Level Permissions . . . 50
Setting Portlet-Level Permissions . . . 51
Setting Resource-Level Permissions . . . 51

Registering a License 53
Using the OMNM Application 53
Using a Command Line Interface 54
Creating an IPv6 Discovery Profile 55
Discovering Resources 58
Tuning Discovery Ping 59
Discovering Your Network 59
Determining Incomplete Discovery 62
Configuring Resync 62
Enabling Zero-Touch Provisioning and Auto-Discovery 63
Resetting a Password 65
Deploying Add-On Capabilities 65
Using Device Drivers 66
Base Driver 66
Supported PowerConnect Models 67
Windows Management Instrumentation (WMI) Driver 67
Web-Based Enterprise Management (WBEM) Driver 68
Optimizing Your System 71
Overriding Properties 71
Tuning Memory (Heap & Portal) 72
Tuning Application Features' Performance Impact 73
Resizing, Starting and Stopping MySQL 73
Maintaining and Repairing Your System 76
Troubleshooting a Balky Application 77
Revising Database Aging Policies (DAP) 78
Reviewing Scheduled Items 78
Backing Up and Administering the Database 78
Cleaning Up Logs 78
Cleaning Up Files 78

2 Configuring the Portal 81
Setting Time Formats 82
Defining a Custom Debug 82
Activating Log4J Email Feature 82
Defining Log4J on Application or Mediation Servers 83
Defining Log4J on Web Servers 84
Hiding Portlet Hint Text 85
Modifying Column Settings 85
Defining Advanced Filters 86
Exporting/Importing Page Configurations 87
Sharing a Resource 87
Editing Custom Attributes 88
Configuring Job Viewer's Appearance 89

Scheduling Actions 90

3 Customizing Events and Alarms 93
Setting Audible Alerts 94
Turning On Audible Alerts 94
Adding Custom MP3 Sounds 95
Creating Event Processing Rules 95
Forwarding Traps 97
Sending as Proxy 97
Forwarding a Generic Message 98
Using Email Action Variables 100
Extracting Adaptive CLI Attributes from a Syslog Alarm 104
Receiving Syslog Events 104
Matching Text from a syslogNotification Event 105
Creating Extended Event Definition for syslogNotification 108
Creating ACLI Action and Pass Varbind Value for Execution 110
Verifying the Results 113
Using Extended Event Definitions 114
Extending Event Definitions 114
Extending Event Definition XML 114
Understanding Alarm Propagation to Services and Customers 119
Understanding Event Life Cycle 122
Understanding Alarm Life Cycle 125

4 Generating Reports 129
Creating a Report Template 130
Generating a Report 131
Branding Reports 132
Adding Custom Report Images 132
Printing Groups of Reports 133
Example Reports 134
Cisco Port Groups 134
User Login Report 135
Network Assessor Reports 136

5 Managing Resources 137
Discovering Resources 138
Modifying Discovery Profiles 139
Logging Terminal Sessions 140
Setting Java Security for Terminal Access 141
Changing Customer to Port Associations 141
Using the Add Ports Action 141

6 Using Visualization Tools 143
Understanding Containers 144
Using Containers 145
Setting Up Google Maps 145
Setting Up Nokia Maps 146
Creating a Topology View 147
Modifying Visualize Label Length 147
Exporting to Visio 148

7 Managing File Servers/Files 149
Understanding FTP/TFTP Servers 150
File Permissions 150
Recommended Windows File Servers 151
External File Server Editor 151
Backing Up Configurations 151
Restoring Configurations 152
Deploying Firmware 154
Restoring a Configuration to Many Devices 154
Creating/Comparing Promoted Configuration Templates 155
Troubleshooting Backup, Restore or Deploy Issues 156

8 Performance Monitoring 157
Best Practices: Performance and Monitors 157
monitorTargetDown Event Interval 160
Monitor Life Cycle 162
Application Server Statistics 167
Resource Monitors 169
Retention Policies 174
Aggregate Data 175
Deployment and Polling of Monitor Targets 176
Monitor Editor 176
Self Management / Self Monitoring: Default Server Status Monitor 185
Monitor Options Type-Specific Panels 196
Bandwidth Calculation 216
Scheduling Refresh Monitor Targets 218
Top N [Assets] 220
Displaying Tenant Domains in Top N Portlets 222
Top Configuration Backups 222
Dashboard Views 223
Performance Dashboard 226
Dashboard Editor 227
Show Performance Templates 232
Multiple Performance Templates 235

Dashboard Templates for Interface and Port Equipment 235
Key Metric Editor 236

9 Traffic Flow Analyzer 239
Best Practices: Performance Tuning Traffic Flow Analysis 240
How does Traffic Flow work? 243
Setup 243
Exporter Registration 247
Traffic Flow Portlet 248
Drill Down 253
Search 254
Traffic Flow Snapshot 255
Settings 255
Domain Name Resolution 257
Traffic Flow Analyzer - Example 257
Traffic Flow Analysis Life Cycle 260

10 Actions and Adaptive CLI 263
Using Adaptive CLI 264
Actions Portlet 265
Adaptive CLI Editor 270
General 270
Attributes 272
Scripts 278
External Executable 284
Seeded External Scripts 287
Adaptive CLI Script Language Syntax 290
Attributes 290
Conditional Blocks 291
Perl Scripts 291
Perl Example 292
Monitoring Upload / Download Speeds 304
Regular Expression Testing 306
Scheduling Actions 307
Comparison 309
Active Performance Monitor Support 309
Action Groups 315
Action Group Editor 315
Troubleshooting Adaptive CLI 317
Adaptive CLI Records Aging Policy 317
Web Service Deployment Features 318

11 Change Management / ProScan 321
Compliance Policy Summary 324
Creating or Modifying a ProScan Policy 325
Creating or Modifying ProScan Policy Groups 339
Standard Policies.....339
Cisco Compliance Policies 340
Cisco Compliance Actions 342
Cisco Event Processing Rules 343
Juniper Compliance Policies 343
Change Determination Process 344
Change Determination Process Workflow 345
Triggering Change Management and ProScan 346
Change Determination Defaults 348
Compliance and Change Reporting 349
Forwarding Configuration Change Commands 350

12 Serving Multiple Customer Accounts 353
Configuring Chat for Multitenancy 353
Configuring Multitenancy, Site Management and Access Profiles 354
Provisioning Site-Creating User Permissions 355
Supported Portlets 357
Site Management 358
Portal > Sites / Site Templates in Control Panel 359
Site Management Editor 363
Access Profile Templates 364
AP Editor / AP Template Editor 365
User Site Access 366
User Site Access Policy 367
Constraining Data Access 368
Manage > Domain Access [Resources] 368
Site ID Filtering 369

13 Troubleshooting Your Application 371
Troubleshooting Prerequisites 371
Mini Troubleshooting 371
Troubleshooting Adobe Flash 372
Database Aging Policies (DAP) 373
Installation Issues 373
Startup Issues 375
Troubleshooting Flow 379
Versions 382

Search Indexes 382
Communication Problems 383
Preventing Discovery Problems 383
Discovery Issues 384
Backup / Restore / Deploy 385
Alarm / Performance / Retention 386
Reports 388
Web Portal 389
MySQL Database Issues 390
Oracle Database Issues 391
Debug 392
WMI Troubleshooting Procedures 395
WMI and Operating Systems 396
WMI Troubleshooting 396
Testing Remote WMI Connectivity 398
Verify Administrator Credentials 398
Enable Remote Procedure Call (RPC) 398
Configure Distributed Component Object Model (DCOM) and User Account Control (UAC) 399
Add a Windows Firewall Exception for Remote WMI Connections 402
WMI Authentication 402
Additional WMI Troubleshooting 402
jstack Debugging in Windows 7 403
FAQs about Monitoring Mediation Servers. 403
Linux Issues 404
Linux syslog not displaying 406
HA installation issue on Linux 407
Device Prerequisites 408
Common Device Prerequisites 408
Aruba Devices 409
Avaya Device Prerequisites 409
Brocade Devices 411
BIG-IP F5 412
Cisco Devices 412
Adaptive CLI FAQs 413
Server Information. 414
Environment / Operating System Issues 415
CRON Events 415
Potential Problem Processes 415
SELINUX 415
Hardware Errors 415
DNS Does Not Resolve Public Addresses 416

Raise User Limits 416
Web Server 416
Clustering 416
Upgrade Installations 417
Patch Installation 417
License Installation 418

14 Localization 419
Localization Overview 420
Adding the Language Portlet 420
Localizing Events 421
Localizing Events not in Event History 423
Localizing Resource Bundles 425
Localizing Message Files 426
Overriding MIB Text for Event Names 427
Caching Message/Property Files 427
Creating Property Files for Double-Byte Characters 428
Understanding the Message Properties Files 429
Producing the Properties List 430
Altering Double-Byte Characters in Audit Trails 431
Setting Up MySQL 431
Setting Up Oracle 431

15 Integrating with Other Dell EMC Products and Services . . 433
Synchronizing with OpenManage Essentials 434
Activating Dell EMC SupportAssist 435
Generating System Performance Summary 438
Configuring Dell EMC Warranty Reporting 439

Appendix A: OpenManage Network Manager User Interface . 441
Portal Overview 442
Menu Options 442
Page Navigation Bar 443
Status Bar 444
General Information 447
Expanded Portlet 450
Settings Window 451
Applications List 453
Password Reminder 453
Home Page 454
Getting Started Portlet 454
Alarms Portlet 454

Managed Resources 454
Quick Navigation Portlet 471
Search by IP or Mac Address Portlet 471
Search by IP or Mac Address 471
Alarms Page 473
Alarms Portlet 473
Expanded Alarm Portlet 475
Alarm Editor 481
Event History Portlet 482
Event History 482
Rule Editor 484
Event Definition Editor 498
Container Manager Portlet 506
Multitenancy and Containers 506
Container Editor 507
Container View Portlet 510
Automation and Event Processing Rules 512
Network Management Page 516
Visualize My Network 516
Visualize Portlet 517
Tools 518
Linked View 521
View 521
Configuring Views 523
Overview Panel 524
Layouts Panel 525
Properties and Settings > Properties 528
Legend Tab 528
Top-Level Nodes Tab 529
Alarms in Visualizations/Topologies 530
Alarm Suppression in Topology Views 530
Links in Visualization 531
Links Portlet 531
New Link 532
Link Discovery 533
Performance Page 535
Top *Asset* Portlets 535
Resource Monitors 537
Dashboard Views 537
Resources Page 538
Managed Resources Portlet 538
Connected Devices Portlet 538

Search by IP or Mac Address 540
Ports Portlet 541
Interfaces Portlet 545
Network Tools Portlet 549
Network Tools 549
Ping Tool 549
MIB Browser Tool 550
Direct Access Tool 550
Discovery Profiles Portlet 552
Discovery Profile Editor 554
Actions Portlet 561
Action Groups Portlet 561
Configuration Management Page 562
Managed Resources 562
Configuration Alarms 569
Configuration Management Schedule 573
Configuration Files Portlet 579
File Management Menu 582
Image Repository Portlet 586
File Servers Portlet 593
Compliance Policy Groups 595
Compliance Policies/Proscan 597
Compliance Schedules 600
Compliance Alarms 604
Equipment Details 608
Reports Page 612
Reports Portlet 612
Report Editor 616
Report Templates Portlet 618
Report Template Editors 618
Settings Page 624
Application Configuration Settings Portlet 624
Language Portlet 625
Common Setup Tasks Portlet 625
Common Setup Tasks Portlet 625
Authentications Portlet 628
Audit Trail Portlet 630
Event Definitions 633
Variable Binding Definitions 635
Variable Binding Definition Editor 636
Managed Resource Groups Portlet 637

Static Group 640
Dynamic Group 641
Vendors Portlet 641
Locations Portlet 644
Locations 644
Contacts 647
Schedules Portlet 649
Application Server Statistics Portlet 652
Site Map Portlet 652
License Viewer 653
License Expiration Notification 654
Product 655
Resource RTM 656
Subscription Information 658
Register License 660
Applications Available for Use 662
Map Context 662
Maps and Containers Together 664
Visualizer Views 665
Cards Portlet 667
Schedule 671
Manage Page 672
Show Versions 672
Control Panel 673
Administrator 674
[Domains] 674
Portal > Users and Organizations 675
Public/Private Page Behavior 676
Portal > Roles 676
Portal > Password Policies 677
Portal > Portal Settings 677
Portal > [Other] 678
Redcell > Permission Manager 678
Redcell > Database Aging Policies (DAP) 681
Redcell > Data Configuration 682
Redcell > Audit Trail Definitions 682
Redcell > Mediation 683
Redcell > Filter Management 685
Redcell > Application Settings 686
Server Administration 689
Audit Trail/Jobs Status 689

Aging Policies Editor 691
Aging Policies Options 693
Sub-Policies 693
Repositories 694

Appendix B: Ports Used 697
Standard Port Assignments 698
Protocol Flows 703
Application Server to Mediation Server Flows 703
JBoss JMS enabled: 703
Application Server to Application Server in Application Server Cluster 704
Application Server to Oracle Database Server 704
Application Server to MySQL Database Server 704
Mediation Server to Application Server Flows 705
Mediation Server to Mediation Server Flows 705
Mediation Server to Network Element Flows 705
Mediation Server to Trap Forwarding Destination 706
Network Element to FTP/TFTP Server 706
Client to Application Server 707
Client to Mediation Server (Direct Access, or Cut thru) 707
Email Network Element Config Differences 708
JBoss Management Access 708
Ports and Application To Exclude from Firewall 708
Firewall Configuration 708
Installed Third Party Applications. 709
Windows Management Instrumentation Ports 710

Index 717

Preface

The Dell EMC OpenManage Network Manager (OMNM) application can give you automated, consolidated configuration and control of your network's resources, even if your resources come from different vendors. You can customize the OMNM, and unify multiple systems for a single view of IT assets, monitoring, compliance auditing, troubleshooting. The OMNM application also communicates with other software systems (like billing or trouble ticketing) in generic WSDL (Web Service Description Language), XML (Extensible Markup Language), and SOAP (Simple Object Access Protocol).

The first chapter of this guide describes security and some of the runtime features supporting these applications. The OpenManage Network Manager *Installation Guide* discusses licensing. Consult Release Notes for information about changes not covered in this Guide.

Why OpenManage Network Manager?

Productive

Discovery and wizard-driven configuration features are available within minutes of OpenManage Network Manager installation, which allow you to discover and monitor your network's devices.

Easy

OpenManage Network Manager provides the network information you need and offers advanced capabilities with minimal configuration overhead.

Valuable

OpenManage Network Manager often costs less to use and maintain than most other solutions.

Scalable

You can scale OpenManage Network Manager to almost any size.

NOTE:

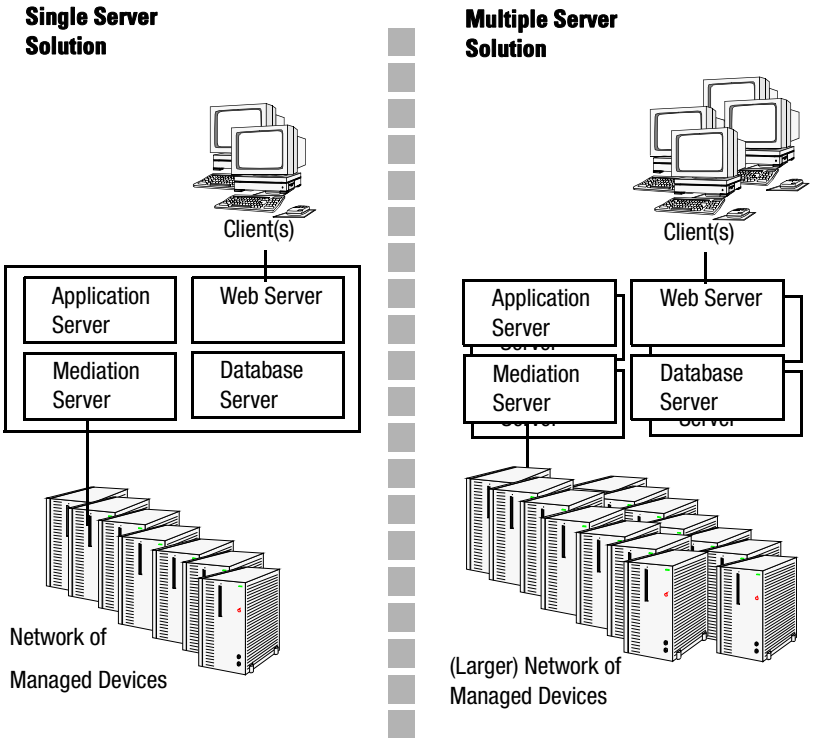
The OpenManage Network Manager product is custom software. The underlying software code, debug statements, installation files, Java classes, license entries, Logs and so on, may refer to names other than OpenManage Network Manager. Such names only have meaning for troubleshooting or support. Most users can safely ignore these. Examples include Redcell, Synergy, Oware, and Liferay.

Application Overview

The OpenManage Network Manager (OMNM) application provides a flexible system to manage networks big and small. It distributes processing between the following elements:

- **Application Server** is the application's "central processor."
- **Web Portal Server** provides clients (browsers) with information based on the Application Server's processes.
- **Mediation Server** manages message processing between the Application Server and managed devices.
- **Database Server** stores and retrieves information about managed devices.

The installation wizard displays these options because you can install each of them to separate servers. Single-server installations are possible. However, to manage larger networks and provide failover High Availability (HA) installations, distributed and redundant installations are also available.



Refer to the *Installation Guide* for more information about distributed and HA installations.

Key Features

The following are some key features of OpenManage Network Manager:

Feature	Description
Customizable and Flexible Web Portal	You can customize the web portal, even providing custom designed views of your data assigned to individual users. You can even create web portal accounts for departments, geographic areas, or other criteria.
Automate and Schedule Device Discovery	Device discovery populates OpenManage Network Manager's database and begins network analysis. You can also create schedules to automatically run Discovery whenever you need to update the initially discovered conditions.
OpenManage Network Manager Administration	You can administer your network—adding devices, user accounts, and web portal displays—from a secure console on your network.
Open Integration	OpenManage Network Manager supports industry standards. It comes with an open-source MySQL database, and supports using Oracle databases. It also uses industry-standard MIBs and protocols, and even lets you install open-source screen elements like Google gadgets to its web portal.
Visualize the Network	The OpenManage Network Manager topology screen lets you create multi-layered, customizable, web-based topology displays of your network to help track the state of network devices.
Alarms	Alarms respond to hundreds of possible network scenarios by default, and you can configure them to including multiple condition checks. Alarms help you recognize issues before your network's users experience productivity losses. Alarms can also trigger actions like e-mailing technical support staff, executing Perl scripts, paging, emitting SNMP traps to other systems, Syslog messaging, and executing external application.
Traps and Syslog	OpenManage Network Manager lets you investigate network issues by examining traps and Syslog messages. You can set up events/alarms and then receive, process, forward, and send syslog and trap messages.
Reports and Graphs	This application comes with many pre-configured reports to display data from its database. You can archive and compare reports, or automate creating them with OpenManage Network Manager's scheduler. If your package includes them, you can also configure graphs to present performance and traffic flow data.
Modularity	Modules analyze network traffic, manage services and IP address and subnet allocations. OpenManage Network Manager modules save time adding to existing OpenManage Network Manager deployments to add feature functionality without requiring additional standalone software.

Networks with Dell EMC OpenManage Network Manager

The beginning of network management with OpenManage Network Manager is executing Discovery Profiles to discover resources on a network. After that occurs, you can configure Visualize My Network (topology views), Resource Monitors, and Performance Dashboards.

After these initial steps, OpenManage Network Manager helps you understand and troubleshoot your network's conditions. For example: Suppose a OpenManage Network Manager Performance Dashboard displays something you want to troubleshoot. You can right-click the impacted device in the Managed Resources portlet to access its configuration and initiate potential actions on it. The Network Status icon in the view indicates the device status. Its Connected Devices panel also displays the highest severity alarm on the device or its sub-components. For example, red indicates a *Critical* alarm.

In screens like Connected Devices Portlet on page 538 you can examine each section of device information and right-click components to see further applicable actions. For example, right-click to Show Performance, and edit and/or save that view of performance as another Performance Dashboard. Performance can also appear in portlets that Show Top Talkers (the busiest devices) or Show Key Metrics.

From looking at Performance Dashboards or Top N [Assets] you may conclude some configuration changes made memory consumption spike. Right-click to access resource actions under File Management Menu that let you see the current configuration files on devices, and compare current to previous. You can also back up devices (see Backing Up Configurations on page 151) and restore previously backed up files (see Restoring Configurations on page 152). Finally, you may simply want to Resync (another right-click menu item) to insure the device and your management system are up-to-date.

NOTICE

Alternatively, the Alarms portlet also lets you right-click to expose Alarm Actions.

You can right-click for Direct Access – Telnet or Direct Access – MIB Browser to display a command line telnetting to the device, or an SNMP MIB browser to examine SNMP possibilities for it.

Click the plus in the upper right corner of any portlet to see its expanded version, for example: the Managed Resources expanded view. This displays detail or “Snap-in” panels at its bottom, with additional information about a selected resource.

Generating a Report let you take snapshots of network conditions to aid in analysis of trends, and Audit Trail portlets track message traffic between OpenManage Network Manager and devices.

Additional Products

The following describes how to increase the power of your OpenManage Network Manager installation. While the OpenManage Network Manager documents describe everything available with the product, your installation may provide only a limited set of those features.

Updating Your License

If you have a limited license — for example OpenManage Network Manager may limit discovery to a certain number of devices — then it does not function outside those licensed limits.

You can purchase additional capabilities, and can update your license for OpenManage Network Manager by putting the updated license file in a convenient directory. Click *License Management* from the Settings > Application Configuration Settings portlet to register your license Your updated license should be visible in the *License Viewer* (See License Viewer on page 653 for details.)

NOTE:

If you update your installation from a previous one where you upgraded license, you must also install any new licenses.

If you import a license that, for example, changes the application's expiration date, it often does not immediately take effect. Log out and log in again to have newly licensed capabilities immediately (with a few exceptions that may make you wait).

Licenses support three expiration formats: *Never*, *Date certain*, and a format that indicates the license will be valid for *a number of days after registration*.

Online Help/Filter

Access general online help by clicking *Help* from the OpenManage Network Manager portal header. Help appropriate to each portlet appears when you click the help tool (question mark) on the portlet title bar.

By default, this opens a separate browser window, which is not necessarily always in front of the screen that calls it. Because it is separate, you can arrange the display so the help screen does not conceal the portlet it describes. Click the *Show* button to display the contents, index and search tabs (*Hide* conceals them again), and the *Prev/Next* buttons, or clicking table of contents topics moves to different topics within the helpset.

NOTICE

A browser's cache may interfere with help's correct appearance. If you see a table of contents node without contents, refresh (Reload) the help window or the application page.



A Note About Performance

OpenManage Network Manager is designed to help you manage your network with alacrity. Unfortunately, the devices managed or the networks that communicate with those devices are not always as fast as this software. If discovery takes a long time (it can), often network and device latency is the culprit. You can also optimize installations to be faster (see the recommendations in the *Installation Guide* and the first chapter of this guide), and limit device queries with filters, but device and network latency limit how quickly your system can respond.

NOTICE

If you use management systems other than this one, you must perform a device level resync before performing configuration actions. Best practice is to use a single management tool whenever possible.

Guide Revision Record

The following log shows revision history for this guide. Refer to the *Release Notes* for a detailed list of features/enhancements.

Date	Version	Description
Oct 15, 2017	6.5.0	Initial release.

1

Getting Started

The section outlines the steps in a typical OpenManage Network Manager (OMNM) installation. Because the software described here is both flexible and powerful, this section does not exhaustively describe all the details of available installations. Instead, references are made to those descriptions elsewhere in this guide, the *OpenManage Network Manager Installation Guide*, or online help. This guide assumes that the OMNM product is installed and operational.

This section focuses on the tasks a user performs. For a detailed description of the OMNM portlet, windows, portlets, options, features, and so on, see OpenManage Network Manager User Interface on page 441.

The following administrative tasks are covered in this section:

General Information – 24
Starting/Stopping OMNM – 27
Setting Up Secure Connections (SSL & HTTPS) – 28
Managing Users and Permissions – 31.
Implementing DAP – 38
Opening an Archive in dapviewer – 39
Backing Up the Database – 39
Restoring Databases – 40
Setting Up Authentication – 41
Configuring Pages and User Access – 48
Registering a License – 53
Creating an IPv6 Discovery Profile – 55
Discovering Resources – 58
Resetting a Password – 65
Deploying Add-On Capabilities – 65
Using Device Drivers – 66
Optimizing Your System – 71
Maintaining and Repairing Your System – 76

General Information

The following topics provide some general information you may need to know:

- Web Portal/Multitasking
- Cookies and Sessions
- Web Clients
- Network Basics

Web Portal/Multitasking

You can open multiple tabs to different managers in the OpenManage Network Manager system. In most cases this does not cause any issues for read–only data browsing. However, **best practice** is not opening multiple tabs when creating, editing or deleting. These may report Web session information incorrectly and task completion may appear to never finish. For example, you may submit a job that appears stuck "running" when in reality it has already finished but the status has not updated in the browser session. When this occurs, manually click the refresh button on the job status window to force an update. The recommended process is to close the job status window and move on to other tasks. The *My Alerts* feature in the portal's lower left corner indicates when jobs are complete, and you can view details from that status bar location.

Cookies and Sessions

The OpenManage Network Manager (OMNM) application stores cookies during the session. No personal data, such as username/password is stored. The cookie stores the assigned session ID as well as information about the current view so that the OMNM application can do partial view updates. OMNM sessions are not persisted, they are in memory only.

Web Clients

With the minimum hardware for a 32-bit client, you can run **either** a Web client or Java client, **not both**. You can start and stop the client without impacting the application server. Device monitoring stops when you stop the application server or turn off its host machine. The client can also be on a different machine than the application server.

NOTE:

See Starting Web Client on page 28 for more information about using web access to this software.

The OpenManage Network Manager (OMNM) application detects mobile devices and pads, such as tablets and iPads. For smaller screens, the Navigation bar collapses to the left hand side and the page only displays a single column. Some limits apply:

- Because touch devices do not support a right-click, the first time clicking a row selects it. A repeat click launches a menu displaying the available actions. Click the menu item you want.
- All major charts are rendered as HTML 5, which are mobile-friendly. These charts are Line, Pie, Donut, Bar and Column. Some Gauges and LED charts require flash, which is not compatible with all mobile devices.

- Topology views are not available.

NOTE:

Apple products are most OpenManage Network Manager-friendly. Android is only partly supported.

CAUTION:

If your application server and client are on different machines, make sure that they have the same time settings.

Network Basics

The OpenManage Network Manager (OMNM) application communicates over a network. In fact, the machine where you install it must be connected to a network for the application to start successfully. Firewalls, or even SNMP management programs using the same port on the same machine where this software is installed can interfere with communication with your equipment.

Dealing with any network barriers to communicating with the OMNM application, any required initial device configuration to accept management, and managing security measures or firewalls—all are outside the scope of document. Consult with your network administrator to ensure this software has access to the devices you want to manage with TCP/IP, SNMP, HTTP/S, UDP Multicast protocols that the OMNM uses.

NOTICE

One simple way to check connectivity from a Linux or Windows machine to a device is to open a command shell (Start > Run `cmd` in Windows). Then, type `ping [device IP address]` at the command line. If the device responds, it is connected to the network. If not, consult your network administrator to correct this. No useful information comes from disconnected or powered-down devices.

Refer to the *OpenManage Network Manager Installation Guide* for additional information about handling disconnected devices and other issues.

The following sections describe:

- Equipment Name Resolution
- Fixed IP Addresses
- Partition Name Limitations

Name Resolution

The OpenManage Network Manager (OMNM) server requires equipment name resolution to work completely, whether done by host files or domain name system (DNS). The application server cannot respond to hosts with IP addresses alone. The application server might not even be in the same network and therefore the host would be unable to connect.

If your network does not have DNS, you can also assign hostnames in `%windir%\System32\drivers\etc\hosts` on Windows (`/etc/hosts` in Linux). Here, you must assign a hostname in addition to an IP address somewhere in the system. Here are some example hosts file contents (including two commented lines where you would have to remove the # sign to make them effective):

```
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
127.0.0.1       localhost
```

Fixed IP Address

OpenManage Network Manager includes a web server and application server which you must install to hosts with fixed IP addresses or permanently assigned Dynamic Host Control Protocol (DHCP) leases. If you have multiple network interface cards, each NIC's IP address must correspond to a different hostname. **Do not** map several NICs with different IP addresses to a single hostname.

If you need to change your host's IP address, do so by:

- Changing Your Host's IP Address using the ipaddresschange script
- Manually Changing Your Host's IP Address

Changing Your Host's IP Address

Change your host's IP address as follows.

1. Change the Virtual host IP to the new IP address in Manage > Control Panel > Portal.
2. Change the host IP address
3. Open a shell and run `oware` to set the environment
4. Run `ipaddresschange -n` in the shell followed by the new IP address
5. Restart the application server and the web server service.
6. Open a browser to see the web client at this URL: `[new IP address]:8080.`

Manually Changing Your Host's IP Address

Change your host's IP address without the `ipaddresschange` script as follows.

1. Change the Virtual host IP to the new IP address in Manage > Control Panel > Portal.
2. Change the host IP address
3. Delete the contents of `\oware\temp`.
4. Change your local IP address anywhere it appears in `\owareapps\installprops\lib\installed.properties`.
5. Change the address on your web server. Change this in `portal-ext.properties` in `\oware\synergy\tomcat-7.0.40\webapps\ROOT\WEB-INF\classes`

   Change property:

   ```
   jdbc.default.url=jdbc:mysql://[IP address]/
       lportal?useUnicode\=true&characterEncoding\=UTF-
       8&useFastDateParsing\=false
   ```

   and

   ```
   oware.appserver.ip=[IP address]
   ```

6. Restart the application server and the web server service.
7. Open a browser to see the web client at this URL: `[new IP address]:8080.`

Partition Name Limitations

First character must be a letter (a-z, A-Z). The remaining must be alphanumeric or underscore or dash characters (a-z, A-Z, 0-9 and _ or -). Maximum length is 31 characters.

In a clustered installation, make `oware/synergy/data` a shared directory because local user images, documents, and uploads go there, and in a cluster environment all web servers need to access this directory.

Starting/Stopping OMNM

The OpenManage Network Manager (OMNM) Application server processes network information for Web-based clients. The Application server monitors devices, and produces the output for the Web server and then makes it available for the Web clients. When you install or upgrade the OMNM application, the installer automatically stops the servers before installation and starts them after installation. However, there are many instances where you need to stop/stop the servers. The following tasks show how to start the Application server and its subordinate process, the mediation server, which communicates directly with devices, and how to stop these processes when needed:

- Starting/Stopping Servers
- Starting Web Client

Starting/Stopping Servers

The following summary shows the various ways to start (and stop) OpenManage Network Manager elements:

Windows Start Menu Program Shortcut	Windows Command Line	Linux Command Line
Server Monitor	pmtray	N/A
Start Application Server	startappserver	startappserver
Network Manager	startsynergy.com **Note:** this is in the oware\synergy\tomcat*\bin directory, and is not on the path.	While no monitor display appears, you can start the Web server with these commands: startportal.sh start/ startportal.sh stop
Web Client	http://[application server host IP]:8080	http://[application server host IP]:8080

From a Windows system, you have several methods to start the **Application server**:

- Select Start > OpenManage Network Manager > Start Application Server.
- Run `startappserver` from a command line tool.
- Right-click the appserver tool in the system tray and then select Start.

NOTE:

My Alerts displays the "Application server is now up" message when application server startup is complete. You can also make server monitor appear with the `pmtray` command either in a shell or from a start menu icon.

If the **Web server** does not start automatically, start it manually

- From a Windows system using one of the following methods:
  - Select Start > OpenManage Network Manager > Synergy Web Service Manager.
  - Right-click the Network Manager tool in the system tray and then select Start.

    If you double-click the Network Manager tool, you can automat the we server startup.
  - Enter the following from the command line:

    installDir`\oware\synergy\tomcat*\bin\startsynergy`
- From a Linux system enter the following from the command line:

  `/etc/init.d/synergy start`

Stop web server by entering `/etc/init.d/synergy stop`

CAUTION:
If your OpenManage Network Manager (OMNM) environment has a firewall, ports 8080 and 80 must be open for it to function correctly. If you want to use cut-thru outside of your network, then ports 8082 – 8089 must be open. The OMNM application uses the first available port, typically 8082. However, if another application uses port 8082, the OMNM application uses port 8083 (if available), and so on. Web Services for the OMNM application uses port 8089 (previous versions used port 80). See Ports Used on page 697 for a complete list of all ports impacted.

Starting Web Client

Open the Web client user interface from your browser. Refer to the *OpenManage Network Manager Installation Guide* for supported browsers and versions. The URL is:

`http://[application server hostname or IP address]:8080`

The default login user is *admin*, with a password of *admin*. The first time you log in, you can select a password reminder. If you have forgotten your password, click the Forgot Password link in the initial screen to begin a sequence that concludes by mailing your user's e-mail address a password. (See Resetting a Password on page 65.)

For this forgotten password sequence to work, you must configure users' e-mails correctly, and the portal's SMTP server in Go to > Control Panel > Server > Server Administration > Mail settings. To configure a user's e-mail settings and other things, click the user name link in the portal header. The same configuration settings are available in Control Panel's tabs labeled as that user's login.

The default login user is *netgear*, with a password of *netgear*.

The *application server hostname* is the name of the system where OpenManage Network Manager is installed.

CAUTION:
The first time you start the application after you install it, you may have to wait an additional five minutes for the Application to completely start. One indication you have started too soon is that the Quick Navigation portlet does not appear properly. **Also:** The Web server may indicate it has fully started before it is entirely ready. In rare instances, this may also inhibit correct communication with the client interface. If OpenManage Network Manager appears stuck after the application server is running completely, restart the Web server.

Disable password reminders with `users.reminder.queries.enabled=false to oware\synergy\tomcat-x.x.xx\webapps\ROOT\WEB-INF\classes\portal-ext.properties`

Setting Up Secure Connections (SSL & HTTPS)

The following describes how to turn on SSL support within OpenManage Network Manager on single-server installations. Configure Clustered installations with a Load Balancer with SSL Offloading. SSL Offloading takes advantage of hardware which has been designed to deal with quick encryption and decryption of SSL. It also lets you purchase a single SSL certificate rather than generating a certificate per server, something that can be more costly.

NOTICE

If you want a secure connection between distributed servers (application and mediation servers, for example), the following also applies.

Set up secure connections (SSL and HTTPS) by:

- Enabling Secure SSL
- Turning on SSL Within the Web Portal

Enabling Secure SSL

Best practice for a clustered production environment is to use a Load Balancer with SSL Offloading rather than creating a private key, as described below. Refer to the *Installation Guide* for more about load balancing.

The private key and certificate described below provides identity and browser verification against the CA signed root certificate. For testing and internal use you need this step to create a Private Key and Private Signed Certificate to enabled SSL encryption.

NOTE:

Some functions may fail using this approach since some third party layers may expect a valid CA signed root.

Enabling secure SSL involves:

- Creating a Private Key (Linux/Windows)
- Creating a Certificate (Linux/Windows)

Creating a Private Key (Linux/Windows)

1. Open a command prompt in Windows or a Terminal within Linux
2. Navigate to a `<INSTALL DIR>/oware/synergy/tomcat-XX/bin/certs`
3. Enter the command: `openssl`

   If this command does not find openssl, then first enter the oware environment (in Windows type `oware`, in Linux, type . ./etc/.dsienv).
4. The OpenSSL prompt appears: `OpenSSL>`
5. Enter the command:

   ```
   genrsa -des3 -out tomcatkey.pem 2048
   ```
6. OpenSSL then asks for a pass phrase for the key. Enter `changeit`. See Turning on SSL Within the Web Portal on page 30 if you want to change the default password.
7. OpenSSL then creates the private key and stores it in the current directory

Creating a Certificate (Linux/Windows)

Once you have the private key created, you must create a certificate.

1. Assuming you are still running the OpenSSL program from the previous step, enter the command:

   ```
   req -new -x509 -key tomcatkey.pem -out tomcat.pem -days 1095
   ```
2. OpenSSL asks for the pass phrase defined for the private key. Enter the previous pass phrase (default: `changeit`). This command creates a self-signed certificate with a lifetime of 3 years, using the private key.

   This password must be identical to the one entered in the previous steps.

3 When asked the other questions such as Country Code, Organization you can enter any data you wish. When asked for the Common Name (FQN) you must enter the hostname or IP address of the server.

4 OpenSSL generates the `tomcat.pem` in the directory you were in from the previous steps.

5 Exit OpenSSL by typing `exit`

6 Two new files appear within the `//../tomcat-xx/bin/certs` directory: `tomcatkey.pem` and `tomcat.pem`

Some systems may put these files in another directory (for example `C:\users\[username]` on Windows 7). If so, copy or move them to the `oware\synergy\tomcat-7.0.40\bin\certs` directory before proceeding.

Turning on SSL Within the Web Portal

The OpenManage Network Manager application is not vulnerable as shipped. If the client does not have SSL turned on with a valid certificate then the following does not matter:

When running Linux, your system admin must keep OpenSSL up to date. This is native to Linux, not to the OpenManage Network Manager application.

For Windows systems, the OpenManage Network Manager application ships with 0.9.8d which is not affected. You can update this any time. This is only applicable if you are using SSL by replacing the openssl.exe file in the oware/synergy/tomcat-xx/bin/native/windows/x64 directory.

Turn on SSL within the Web portal by doing what applies for your operating system:

- Changing the Windows Environment
- Changing the Linux Environment
- Enabling Terms of Use

Changing the Windows Environment

First, update the `setenv.bat` with the SSL preferences. You must do this whether OpenManage Network Manager's web server starts manually or runs as a service. if OpenManage Network Manager runs as a service, this file automatically updates the service on the next portal service restart.

1 Stop OpenManage Network Manager service

2 Navigate to the `<INSTALLDIR>/oware/synergy/tomcat-xx/bin` directory.

3 Edit the `setenv.bat` file in a text editor.

4 Change the property `ENABLE_SSL=false` to `ENABLE_SSL=true.`

5 If you used a pass phrase different from `changeit` then you can set it for the `SSL_PASSWORD=changeit` value.

6 Save `setenv.bat`

7 In a command prompt navigate to `/oware/synergy/tomcat-xx/bin`, and type: `service.bat update`

8 Settings take affect after the you restart the service.

You are now ready for a secure, SSL connection to OpenManage Network Manager. After it has had a few minutes to start navigate to `https://[application server IP address]:8443.` (The HTTPS port is 8443, not 8080.)

Changing the Linux Environment

1. Enter the command: "`service synergy stop`" to stop the OMNM service.
2. Navigate to the `/oware/synergy/tomcat-xx/bin` directory
3. Edit the `setenv.sh` file.
4. Change `ENABLE_SSL` to `true`.
5. If you used a different pass phrase than the default (`changeit`) then you can set it for the `SSL_PASSWORD` property here.
6. Save the file.
7. `Enter the command: "service synergy start" to restart the OMNM service.`

You are now ready for a secure, SSL connection to OpenManage Network Manager. After it has had a few minutes to start navigate to `https://[application server IP address]:8443`

Enabling Terms of Use

To Enable a "Terms of Use" statement required of each user use the following steps:

1. Login as Admin
2. Go to Control Panel
3. Click on Portal Settings and then the Users link on the right, and look in the Fields tab.
4. Check *Terms of Use Required* and save. You must then click *I Agree* to the Terms of Use document that appears.
5. Logout and attempt to login as another user to validate the Terms of Use appear.

To change the Terms of Use wording:

1. Login as Admin
2. Go to the Synergy Control Panel
3. Click on Web Content
4. Click on the TERMS-OF-USE article link which will take you to the editor where you can alter and save it.

NOTE:

Nothing prevents a user from deleting the Terms of Use article. If the Terms of Use seeded article is removed then the static Liferay Terms of Use appears until next OpenManage Network Manager restart. The editable/delete-able article is a copy of the compiled static version but exposed as an article to make editing easier. The next time OpenManage Network Manager restarts, if the TERMS-OF-USE article does not exist, it imports a new one.

Managing Users and Permissions

This section provides the following tasks to manage users and their permissions:

- Adding Users and Connecting them to Roles
- Adding and Configuring User Roles/Permissions
- Adding Individual Permissions
- Adding LDAP Users
- Creating an LDAP Admin User

Adding Users and Connecting them to Roles

When you add a new user, that user may not appear immediately. You can speed up the user's appearance by using control panel's *Server* > *Server Administration Resource* panel. Click *Reindex all search indexes*.

Add Users with the following steps:

1 Click *Go to* > *Control Panel* and navigate to Portal > Users and Organizations.

2 Click the *Add* > *User* menu item at the top of the *Users* screen.

3 Enter the details of the new user. If you are editing an existing user, more fields appear. *Screen Name*, and *Email Address* are required. Optionally, you can enter *Name*, *Job Title*, and so on.

NOTE:

Make sure you specify a *Password* when you add a user. This is not optional.

4 After you click *Save* notice that the right panel expands to include additional information.

The first time users log in, the application prompts them for a security question. E-mail for password reminders/resets requires setting up the fields in Control Panel > Server Administration > Mail, not the SMTP Configuration which is for OpenManage Network Manager-originated e-mails. See Resetting a Password on page 65

Also: When you make a multitenant site, OpenManage Network Manager automatically assigns the site prefix you select to the admin user it creates in the Site Management Editor. If you enter "Admin" as that user, and the prefix is DS-, then that user must log in as "DS-Admin." When you or the tenant site admin create tenant site users manually in control panel, you must manually add that prefix too when creating the user and when logging in as that user.

5 Notice that if you are editing an existing user, or creating a new one, you can use the links on the right to configure connections with *Roles*. Roles, in particular, configure the OpenManage Network Manager functional permissions for that user. For example the *Operators* role's capabilities are typically more limited than *Administrators*. See Adding and Configuring User Roles/Permissions on page 34.

6 Click *Save* again, and the user you just configured should appear listed in the *Users* screen when you select *View* > *All Users*.

7 After you have configured roles as described in Adding and Configuring User Roles/ Permissions on page 34, return to the Users and Organizations screen, edit the User, and click the *Roles* link to associate the User with the Roles you have configured.

The most dramatic evidence of permission changes appears when you first remove Default User Roles — Power User from your system in Portal > Portal Settings > Users > Default User Associations (check *Apply to Existing Users* if you have already configured your user). If you impersonate your user, and Go To > Control Panel, without User and Power User roles assigned, the impersonated user can only see *My Account* and *Sites*.

NOTICE

You can *Export Users* to a comma-separated value (CSV) file.

Once you have configured a user, you can click *Action* and to do the following:

Edit—Re-configure the selected user. Select the user's Role in the editor, too. Roles configure access and action permissions.

Permissions—Manage the user's access to and control over various parts of the portal.

Impersonate User (Opens New Window or tab)—This allows you to see the effect of any configuration changes you have made on a user. The new window (typically a new tab) also lets you click the *Sign Out* link in the upper right corner where you can return to your original identity impersonation concealed.

Manage Pages—The menu described below appears when you have not installed the Multitenancy option. Configure the *Public* or *Private* pages for a user, depending on the selected tab. Possible actions here include changing the look and feel of pages (for computers and mobile browsers), adding pages and child pages, and importing or exporting page configurations. Notice that you can configure meta tags, and javascript on these pages too.

Exports are in `.lar` format, and go to the download location configured in the browser you are using. The export screen lets you select specific features, and the date range of pages to export.

NOTICE

If you want to set up several pages already configured elsewhere for another user, or even for an entire community of users, export those pages from their origin, then *Manage* > *Pages* menu for the user or community.

Also: On private pages, you can see the *Languages* portlet. Click a flag to translate some labels to the language represented by the flag. You can change the text in many labels (the portlet titles, for one example) by clicking and re-typing that label. Some labels do not translate, no matter what.

See also the Multitenancy chapter of the *Installation Guide* for more potential variations on page appearance.

Deactivate—Retires a user configured on your system. You can also check users and click the *Deactivate* button above the listed users. Such users are not deleted, but are in a disabled state. You can do an Advanced search for inactive users and *Activate* them or permanently delete them.

Your organization has a number of geographic locations and you plan to manage the network infrastructure for all these locations using RC7 Synergy. You can define the geographic locations to which devices can be associated. This will help you manage and view your network, grouped by location or branches. See Locations Portlet on page 644 for the specifics about the portlet where you can set up locations.

NOTICE

To edit your own information as a signed-in user, simply click your login name in the upper right corner of the portal screen.

Organizations

Create Organizations just as you would create Users. You can create a *Regular* or *Location* type of organization. You can do this only if your package includes the MSP option, so this capability is not available to all users.

NOTE:

You must first create a *Regular* organization to be the parent for a *Location*. **Also:** These organizations are useful to organize users. They are distinct from the device-organizing Locations described in Locations Portlet on page 644, and are not available for organizing in Containers (see Using Containers on page 145).

Adding and Configuring User Roles/Permissions

Add and configure User Roles with the following steps:

1. Click Go to > Control Panel > Portal > Roles.
2. Click the *Add* tab under the heading at the top of the page, and select Regular *Roles*.

   The New Role options are displayed.

   You can also add site and organization roles that configure permissions.
3. Enter the details of the new role (*Name*, *Title*, *Description*), then *Save* it.
4. Click Portal > Roles > *View All* to verify that the new role was added to the list.

   The actions available for a new role are Edit, Permissions, Define Permissions, Assign Members, View Users, and Delete role.
5. Click Actions > Define Permissions for the new role.

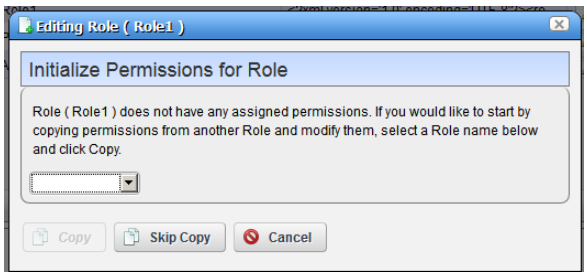
   The Define Permissions editor is displayed.

   Alternatively, select or delete OpenManage Network Manager permissions by editing the role in *Redcell* > *Permission Manager*.

NOTE:

If you are restricting permissions for new users, you must also remove the permissions from the *User* and *Power User* roles, that OpenManage Network Manager assigns all new users by default. The permissions available are a combination of those configured here and the User *and* Power User roles' permissions. You can remove users from the Power User role altogether, but not from the User role. You must remove permissions from that User role if you want users not to have them.

If you have eliminated all permissions from a role by removing the Default User Roles — Power User, an intervening screens lets you copy another Role's permissions so you do not have to enter all permissions from scratch.



NOTICE

Defining a base role's permissions can provide the start for non-base role's permissions if you use this screen to copy them, then edit them later for the difference between the base role and non-base role. As always, planning is the key to simplifying this work.

6. Select the type of permission from the Add Permissions list.
7. Select the actions you want to enable.
8. Click the Redcell > Permission Manager to alter or enable more of OpenManage Network Manager functional permissions.

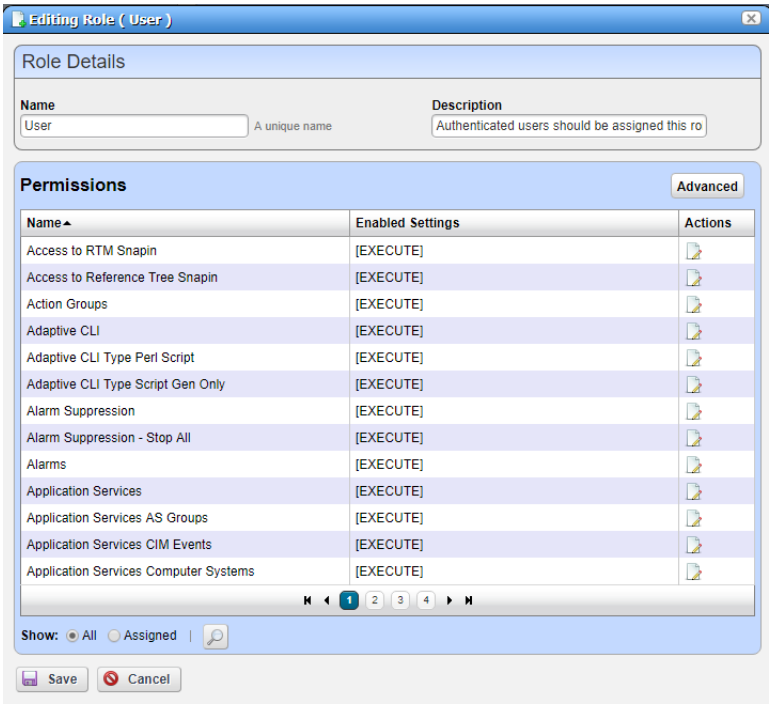
   The Role to Permission Settings list is displayed.

9 Click the action's Edit button to see and configure available permissions.

The Editing Role window is displayed.

NOTICE

The Show Assigned/Show All options to filter what displays in the list.



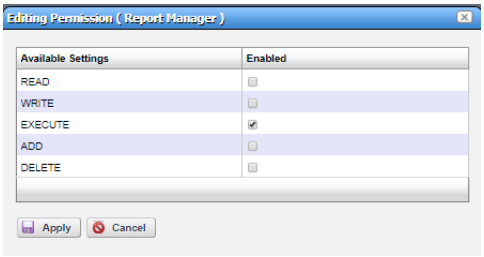
10 Click *Advanced* to see available permissions organized by *Read*, *Write*, *Execute*, *Add* or *Delete* actions.

11 Select the appropriate permissions for each category.

12 Apply your changes.

13 Click the action's Edit button to modify permissions type.

The Editing Permissions window is displayed.

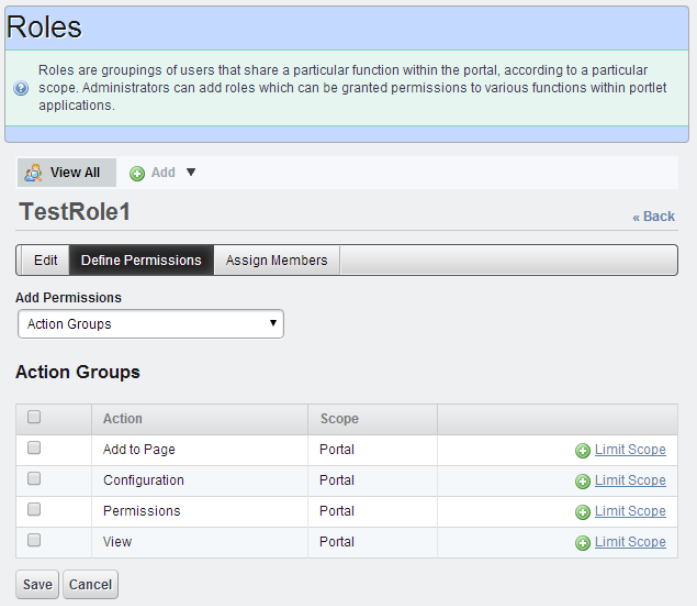


14 Enable and apply the appropriate permissions.

15 Save the role configuration.

Adding Individual Permissions

The Redcell > Permission Manager options are more convenient to do this in bulk, but to add individual permissions, click Portal > Roles > Actions > Define Permissions for the appropriate role, and then select the specific resource set.



Once you select a general type of permission with the pick list below *Add Permissions*, the *Action Groups* that appear below let you check to select areas to enable, and the *Limit Scope* link to the right lets you further filter the application of this enabled permission. The *Private Pages* limitation in this final filter does not apply in Multitenant systems.

Because these screen are so granular, however, best practice is to use them to fine tune existing permission structures.

When you try to log in as a Multitenant Users, OpenManage Network Manager prepends the Screen Name Prefix if you create the user in the Site Management Editor. If you make other users for the tenant site manually in Control Panel, you must manually add the prefix to assign them to the correct site.

Adding LDAP Users

You can integrate LDAP with your OpenManage Network Manager installation in the Portal Settings > LDAP tabs. LDAP-added users cannot log into OpenManage Network Manager's Java Client, and can only use the web portal.

△ CAUTION:

Before enabling an LDAP server in the Portal, you must create and assign one user from the LDAP server as the Portal administrator. You cannot access the Control Panel without a user with the administrator role. See Creating an LDAP Admin User below for details.

Make sure *Import at Startup* is turned off and in Password Policies, edit the default password policy and make sure that *Change Required* is off.

NOTICE

Notice that several test buttons appear in the LDAP screens, for example, *Test LDAP Connection*. Use these to validate your entries as you make them.

Click *Add* under LDAP Servers to add the specifications of your LDAP server. After configuring your LDAP server, restart the OpenManage Network Manager server, and attempt to log in as an LDAP user.

LDAP Server Settings

The following settings are required (the values below are examples, only):

Connection

Base Provider URL : ldap://192.168.50.25:389

Base DN : dc=dorado-exchange,dc=oware,dc=net

Principal: dorado@dorado-exchange.oware.net [Principle user must have the necessary administrator rights in Active Directory Server or any other LDAP server]

Credentials: ********

Users

Authentication Search Filter:(sAMAccountName=@screen_name@)

Import Search Filter: (objectClass=person)

User Mapping

Screen Name: sAMAccountName

In the Portal Settings > Authentication > LDAP tab:

Authentication

Enabled

Import/Export

Import Enabled

Import on Startup Disabled

Creating an LDAP Admin User

All users imported from an LDAP server default to the *Poweruser* role. The default OpenManage Network Manager (login/password: admin/admin) cannot log into Synergy once you enable authentication through LDAP. Therefore, you must manually assign one of the users from the LDAP server as the Portal administrator. An example of an LDAP database user with Administrator privileges:

Screen name: ITAdmin

User password: ITPassword

First Name: Scott

Last Name: Smith

Email: scott@doradosoftware.com

NOTE:

You cannot import users without these five attributes into OpenManage Network Manager from an LDAP source.

Creating user ITAdmin with Administrator role:

1. As an Admin user, *Go to* > *Control Panel*.
2. Under the Portal category, click *Users*, then click the *Add* button.
3. Fill out the User form with name and email address and so on. Remember: screen name, first name, and email address are required. Synergy LDAP import will not overwrite existing users.
4. When you are finished, click *Save*.
5. A message appears saying that the save was successful.
6. Select the Password, enter password: ITPassword and click Save.
7. Click the *Roles* link. A screen appears showing the roles to which your ID is currently assigned. By default, all users are assigned the Power User role.
8. Remove the default PowerUser role (optional), and add the administrator role for the user, then click *Save*.

   Now you can enter LDAP server info.

Stopping LDAP Authentication

1. To stop authenticating through LDAP, log in as the admin user with ITAdmin/ITPassword.
2. In control panel go to *Portal* > *Portal Setting* > *Authentication* > *LDAP* and deselect the *Enabled* then *Save*.
3. When the portal re-appears, Users can login only with credentials that exist on Synergy database

Implementing DAP

Database Aging Policies (DAP) prevent the OpenManage Network Manager database from filling up by filling up by deleting old records. You can also save designated contents to an archive file on a specified cycle. Database Aging Policies configure which contents to archive, the archive location, and the configuration of that archive file.

To view and manage such policies, right click an item with them (for example, an alarm), or click *Manage* > *Control Panel*, and under *Redcell* click *Database Aging Policies*.

Policies appear in the *Aging Policies* tab of this screen, with columns that indicate whether the policy is *Enabled*, the *Policy Name*, *Details* (description), *Scheduled Intervals* and icons triggering three *Actions* (*Edit*, *Delete* and *Execute*). Notice that the bottom right corner of this page also lets you *Enable/Disable/Execute All* policies listed.

Implement DAP from the list of DAPs as follows.

1. Click *Add Policy* and then select a policy from the list of alternatives.

   The Aging Policies Editor is displayed.
2. Select the General tab.
3. Specify the name, schedule interval, whether this policy is Enabled, and so on.

4 Specify the *Archive Location*.

Those listed are the *Repositories* listed on the Repositories panel. You can manage those on that tab.

5 Click the Options tab.

6 Specify either the archiving and retention you want, or further specify sub-policies that refine the items archived, and specify archiving and retention for those sub-policy elements.

Which one you can specify depends on the type of DAP you are configuring.

7 Click Apply until the DAP manager is displayed.

8 View/Verify DAP.

DAP archives information into the specified repository under the installation root. You can open archived .xml data with `dapviewer`. Launch this application from a command line after setting the environment with `oware` in Windows or `. ./etc/.dsienv` in Linux.

Archived data is deleted from OpenManage Network Manager's database. You can verify that by querying whether archived data still exist. You also can backup your database if you want to preserve records not yet archived.

Opening an Archive in dapviewer

1 First, make sure you have an archived file. One way to do this is to edit the Events DAP, make sure the archived events go to a directory you can access later, and retain them for zero days.

2 Manually run the Events DAP

3 Open a command shell. Type `oware` in Windows, or `. ./etc/.dsienv` in Linux.

4 Type `dapviewer.`

5 Select the file with the ellipsis (...).

NOTE:

dapviewer opens both compressed and uncompressed files. It does not open empty files. **Also:** You must have display set to the host running dapviewer if you are running it on a remote host.

6 Click the *Load* button.

7 Examine the archived data.

Backing Up the Database

To back up your database, open a command shell (*Start* > *Run* `cmd`, in Windows), and then type the following at the prompt replacing USERNAME and owbusdb. By default, the database is `owbusdb`, user name is `root` and password is `dorado`.

```
mysqldump -a -u USERNAME --password=[name] owbusdb > FILENAME.mysql
```

For example:

```
mysqldump -a -u oware --password=dorado owmetadb > owmetadb.mysql
```

If you have Performance monitors or Traffic Flow Analyzer, you must also back up your stored procedures otherwise they do not get restored when you restore the database. The command line here adds `--routines`. For example:

```
mysqldump -a -u oware --password=dorado --routines owbusdb > owbusdb.mysql
```

This writes the owbusdb to a plain-text file called `FILENAME.mysql` (`owbusdb.mysql` in our examples). This file is a full backup with which you can fully restore your database in case of problems.

Defaults for the database are `oware` (login) and `dorado` (password). These are typically different from the login/password for the application.

NOTICE

To get a rough estimate of a database's size, looking at the size of the directory `\oware3rd\mysql\data.`

Here are the backup commands for all the databases:

```
mysqldump -a -u root --password=dorado owbusdb > owbusdb.mysql
mysqldump -a -u root --password=dorado owmetadb > owmetadb.mysql
mysqldump -a -u root --password=dorado lportal > lportal.mysql
mysqldump -a -u root --password=dorado synergy > synergy.mysql
```

To backup stored procedures too:

```
mysqldump -a -u oware --password=dorado --routines owbusdb > owbusdb.mysql
```

Restoring Databases

Restoring from `FILENAME.mysql` is a three step process. This occurs, again, in a command shell:

1. Drop the database:

   ```
   mysqladmin -u USERNAME -p drop owbusdb
   ```

   or

   ```
   mysqladmin -u USERNAME --password=[password] drop owbusdb
   ```

2. Recreate the database

   ```
   mysqladmin -u USERNAME -p create owbusdb
   ```

   or

   ```
   mysqladmin -u USERNAME --password=[password] create owbusdb
   ```

3. Import the backup data

   ```
   mysql -u USERNAME -p owbusdb < FILENAME.mysql
   ```

   or

   ```
   mysql  -u USERNAME --password=[password] owbusdb < FILENAME.mysql
   ```

Here are restoration commands for all the databases:

```
mysql -u root --password=dorado owmetadb < owmetadb.mysql
mysql -u root --password=dorado owbusdb  < owbusdb.mysql
mysql -u root --password=dorado lportal  < lportal.mysql
mysql -u root --password=dorado synergy  < synergy.mysql
```

NOTE:

If you receive the error "Access Denied. Invalid Role for this device" or if the applications fails with error indicating that it cannot connect to the device after a network change, There may be a DNS resolution issue. You may still be able to ping or connect to a device by IP address but testing server connectivity by using hostname will confirm or rule out a DNS problem. This would only be a problem if the devices were discovered or set to "Manage by Hostname". If the system was migrated to a system that is not using

DNS, then name resolution could fail and there would be no connectivity to devices. The solution from the Resource Manager is to Right Click -> edit and un-check "Manage by Hostname". This will then default to Manage by IP address. Alternatively, you can fix name resolution in your environment.

NOTICE

Whenever you upgrade your system and your database is on a separate server, you must run the `oraclepostinstall` script on the (primary) application server too.

Setting Up Authentication

The following tasks are related to setting up authentications. The steps you follow depend on which method you choose for authenticating.

- Integrating LDAP
- Configuring a CAS Server with RADIUS
- Setting Up Radius Authentication

Integrating LDAP

You can integrate LDAP with your OpenManage Network Manager installation in the Control Panel > Portal Settings > Authentication > LDAP

CAUTION:

Before enabling LDAP server in Portal, you must create and assign one user from LDAP server as Portal administrator. You will not be able to access control panel without administrator role.

Integrate LDAP by:

- Assigning one user from LDAP server as Portal administrator
- Adding an LDAP server
- Turning off default 'admin' user's local authentication. (Optional)
- Restarting the Web Server

Review the LDAP and Multitenancy FAQs to resolve any questions you might have.

Assigning one user from LDAP server as Portal administrator

All users imported from an LDAP server default to the Poweruser role. The default OpenManage Network Manager (login/password: admin/admin) cannot log into OpenManage Network Manager once you enable authentication through LDAP. Therefore you must manually assign one user from the LDAP server as Portal administrator. Here is an example of an LDAP database user with Administrator privileges:

Screen name: ITAdmin

User password: ITPassword

First Name: Scott

Last Name: Smith

Email: scott@dellhardware.com

NOTE:

You cannot import users without these five attributes into OpenManage Network Manager from an LDAP source.

Create the ITAdmin user with Administrator role as follows.

1 Sign in as an Admin user.

2 Select Go to > Control Panel > Portal > Users.

3 Click the Add button.

4 Fill out the User form with name and email address and so on.

Remember: screen name, first name, and email address are required. OpenManage Network Manager LDAP import will not overwrite existing users.

5 Click Save when done.

A message appears saying that the save was successful.

6 Select the Password, enter password: ITPassword, and then click Save.

7 Click the Roles link.

A screen appears showing the roles to which your ID is currently assigned. By default, all users are assigned the Power User role.

8 Remove the default PowerUser role (optional), and add the administrator role for the user, then click Save.

Now you can enter LDAP server information. Be patient, your changes may take a moment to take effect.

Adding an LDAP server

In the LDAP tab of the Authentication screen, select the *Enabled* option, click *Add* under *LDAP Servers*, and then fill in that screen as appropriate.

Authentication

Enabled

Import/Export

Import Enabled

Import on Startup Enabled

NOTICE

Notice that several test buttons appear in the LDAP screens, for example, *Test LDAP Connection*. Use these to validate your entries as you make them.

LDAP Server Settings

The following settings are required (the values below are examples, only):

Connection

Base Provider URL : ldap://192.168.50.25:389

Base DN : dc=test-exchange,dc=oware,dc=net

Principal: test@test-exchange.oware.net

NOTE:

The Principal user must have the necessary administrator rights in Active Directory Server or any other LDAP server

Credentials: ********

Users

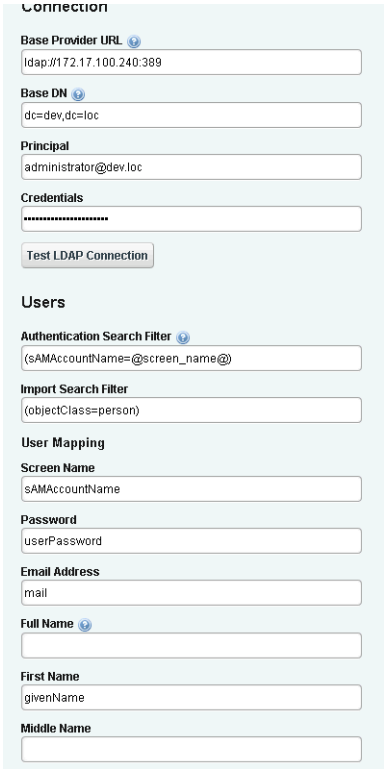
Authentication Search Filter:(sAMAccountName=@screen_name@)

Import Search Filter: (objectClass=person)

User Mapping

Screen Name: sAMAccountName

In the Portal Settings > Authentication > LDAP tab



Turning off default 'admin' user's local authentication. (Optional)

By default, user 'admin' able to login with local authentication even when 'LDAP' required was selected.

To prevent user 'admin' to use local authentication, edit the file .../oware/synergy/conf/server-overrides.properties and add the following line:

auth.pipeline.enable.liferay.check=false

NOTE:

user will need to rename server-overrides.properties.sample to server-overrides.properties

Restarting the Web Server

Restart the OpenManage Network Manager server, and attempt to log in as an LDAP user.

NOTE:

If LDAP users are not imported correctly, you can check the log under .../oware/synergy/tomcat-7.0.40/logs/

LDAP and Multitenancy FAQs

The following are answers to some of the frequently asked questions about LDAP, particularly related to multitenancy.

Disabling logins after a preset number of failed attempts—OpenManage Network Manager supports this for both local and LDAP users.

Reporting login attempts—Supported from report: User Login Report/Last 30 Days.

All users log in with LDAP—This is supported. Tenant site users must prepend the site prefix. For example: The full screen name for user *admin* in customer site with the prefix *BP*, logs in as *BP-admin*.

Are Passwords stored as plain text?—Passwords are stored in encrypted form in the database, even for imported users. LDAP users can authenticate through Active Directory (AD) or OpenLDAP. If you do not want locally stored password, manually create users. Alternatively, import users, then disable import, and change the local passwords so they are different than the one from AD.

Roles and Users—You must locally configure different roles for users within OpenManage Network Manager.

Authentications—By default Redcell authenticates from the local servers. If you add `auth.pipeline.enable.liferay.check=false (in [installation root]\oware\synergy\tomcat-7.0.40\webapps\social-networking-portlet\WEB-INF\classes\portal.properties)` and enable LDAP required, it uses LDAP to authenticate. Liferay does have multiple entries for AD and OpenLDAP.

Configuring a CAS Server with RADIUS

OpenManage Network Manager does not support RADIUS for authentication directly, however it does support LDAP (see Integrating LDAP on page 41), CAS, NTLM, OpenID, Open SSO and SIteminder. If you are not doing NTLM/LDAP/Active Directory, Central Authentication Service (CAS) is a widely used, open source central authentication solution.

NOTE:

This feature imports users with the default level of permissions. You must manually alter permissions and create groups if you want to differentiate between user permissions.

CAS can also use various authentication schemes like LDAP, or RADIUS, so OpenManage Network Manager supports those indirectly. Web applications like OpenManage Network Manager only need to know about the CAS server, not the various authentication protocols CAS uses to provide the final authentication mappings.

One popular CAS Server is available at: http://www.jasig.org/cas

Configure access to CAS in the Portal > Portal Settings > Authentication > CAS tab, which includes a *Test CAS Configuration* button. Other tabs are available here for authentication too, for example LDAP and Active Directory (see Integrating LDAP on page 41 for instructions about how to enable LDAP).

Liferay provides foundation classes for OpenManage Network Manager's web client. Liferay Wiki instructions about setting up CAS appear here: http://www.liferay.com/community/wiki/-/wiki/Main/CAS+Liferay+6+Integration.

The example we tested uses two devices running Tomcat 7.x and Java 6 on one device (DeviceA) and OpenManage Network Manager on the second device (DeviceB). You must access DeviceA using its fully qualified hostname (example: QA002.test.loc, not QA002). You must create `cas-web.war` for OpenManage Network Manager's CAS server to support this. Instructions about how to do this are on the CAS open source site at wiki.jasig.org/display/CASUM/Best+Practice+-+Setting+Up+CAS+Locally+using+the+Maven+WAR+Overlay+Method. Your preferred search engine may find other instructions for compiling or downloading `cas-web.war` file.

Configure a CAS server with RADIUS by:

- Configuring DeviceA
- Creating RADIUS Configuration Setup
- Creating, Exporting, Importing Certificates Using Java

Configuring DeviceA

Follow these steps:

1. Install tomcat 7.x (example: `apache-tomcat-7.0.37-windows-x64.zip`)
2. Insert `cas-web.war` into the `..\tomcat\apache-tomcat-7.0.37\webapps` directory. Start Tomcat (run `startup.bat` in `tomcat\bin` directory). This extracts `cas-web.war`, creating the `cas-web` folder with subcomponents.
3. Shut down Tomcat (`shutdown.bat`)

Creating RADIUS Configuration Setup

Follow these steps (inserting the correct path when `[path]` appears):

1. Edit the `deployerConfigContext` file located in the `..tomcat\apache-tomcat-7.0.37\webapps\cas-web\WEB-INF` directory.
2. Search for the `RadiusAuthenticationHandler` section of that file.
3. Replace index="0" with the IP address of the RADIUS server.
4. Replace index='1' with the global RADIUS server password.
5. We tested a RADIUS server using mschapv2 protocol. If your radius server uses a different protocol replace index='2' value with the correct RADIUS protocol value.
6. *Save* this file.

Creating, Exporting, Importing Certificates Using Java

Follow these steps:

1. Run the following from the Java location on your computer (typically under `c:\Program Files` in Windows):

```
..Java\jdk1.6.0_26\bin>keytool -genkey -alias cascommon -keyalg RSA
..Java\jdk1.6.0_26\bin>keytool -export -alias cascommon -file
    casserver.crt
```

```
..Java\jdk1.6.0_26\bin>keytool -import -trustcacerts -alias cascommon -
    file casserver.crt -keystore "C:\Program
    Files\Java\jdk1.6.0_26\jre\lib\security\cacerts"
```

2 Uncomment `connector port="8443"` section in the `..\tomcat\apache-tomcat-7.0.37\conf\server.xml` file.

3 Add keystorefile, keystorepass, truststorefile properties:

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
               maxThreads="150" scheme="https" secure="true"
               clientAuth="false" sslProtocol="TLS"
keystoreFile="C:\users\TestUser\.keystore"
keystorePass="changeit"
truststoreFile="C:\Program
    Files\Java\jdk1.6.0_26\jre\lib\security\cacerts"
/>
```

4 Comment out the following:

```
<Listener
    className="org.apache.catalina.core.AprLifecycleListener"
    SSLEngine="on" />
```

5 Restart the tomcat server.

6 Copy the `casserver.crt` file that was created during `keytool -export` from deviceA to deviceB.

7 Do the following configuration on deviceB

a. Import the certificate:

```
/cygdrive/c/[path]/oware3rd/jdk1.6.0_45nt64:keytool -import -trustcacerts
    -alias cascommon -file "c:\ssl\casserver.crt" -keystore
    "[path]\oware3rd\jdk1.6.0_45nt64\jre\lib\security\cacerts"
```

b. Add near the end of `set "JAVA_OPTS" -Djavax.net.ssl.trustStore="[path]\oware3rd\jdk1.6.0_45nt64\jre\lib\security\cacerts"` to the `setenv.bat` file located in `..\oware\synergy\tomcat_xxx\bin`

When finish the line should look like this:

```
set "JAVA_OPTS=%JAVA_OPTS% -Dfile.encoding=%PORTAL_ENDCODING% -
    Djava.net.preferIPv4Stack=%PORTAL_IP_STACK% -
    Dsynergy.https=%ENABLE_SSL% -Dssl.certfile=%SSL_CERTFILE% -
    Dssl.certkeyfile=%SSL_CERTKEYFILE% -Dsynergy.http.port=%PORTAL_PORT% -
    Djavax.net.ssl.trustStore="[path]\oware3rd\jdk1.6.0_45nt64\jre\lib\sec
    urity\cacerts" -Xms%PORTAL_MAX_MEM% -Xmx%PORTAL_MAX_MEM% -
    XX:MaxPermSize=%PORTAL_PERMGEN%"
```

c. Edit deviceB's `portal-ext.properties` file located in:

`\oware\synergy\tomcatxxx\webapps\root\web-inf\classes`

d. Set property settings as follow:

```
live.users.enabled=false
com.liferay.portal.servlet.filters.sso.cas.CASFilter=true
default.landing.page.path=/group/root
company.default.home.url=/group/root
```

8 Restart web service using a command window to run this command:

```
oware/synergy/tomcat-7.0.40/bin/startup.bat
```

9 Go to > Control Panel in OpenManage Network Manager

10 Select *Portal* > *Portal Settings*

11 Click on the *Authentication* link on the right

12 Click the CAS tab.

13 Select the *Enabled* option.

14 Change the login URL to:

```
https://deviceA_hostname:8443/cas-web/login
```

15 Change the logout URL to:

```
https://deviceA_hostname:8443/cas_web/logout
```

16 Change the server URL to:

https://deviceB_IPAddress:8443/cas_web

17 Click the Test CAS Configuration button.

18 Click Save, if the test passed.

19 Create users (no password) that already exist on the RADIUS server from the Go to > Control Panel > Portal > Users and Organizations options.

This allows you to use RADIUS with the OpenManage Network Manager application.

20 Sign out from the OpenManage Network Manager portal.

21 Enter your OpenManage Network Manager:8080 URL from a browser.

A CAS authentication page is displayed.

22 Enter credentials of users created on radius server.

Setting Up Radius Authentication

The OpenManage Network Manager (OMNM) application supports radius authentication using an external radius authentication server. To set up direct radius support, you need an OMNM user with the same name as the radius user name.

Set up direct radius support as follows.

1 Configure the OMNM system to recognize your radius server.

a. Navigate to the installDir/owareapps/installprops/lib/installed.properties file.

b. Open the installed.properties file with a text editor.

c. Add the following properties:

```
com.dorado.server.radius.server=<serverIP>  required
com.dorado.server.radius.port=<radius port#> optional, default = 1812
com.dorado.server.radius.secret=<radius secret value> required
com.dorado.server.radius.timeout=<timeout in ms> optional, default =
    1000 ms
```

For example:

```
com.dorado.server.radius.server=192.168.54.137
com.dorado.server.radius.port=1812
com.dorado.server.radius.secret=testing123
com.dorado.server.radius.timeout=1000
```

2 Enable radius authentication.

a. Navigate to the *installDir*/oware/synergy/tomcat-7.0.40/webapps/netview/WEB-INF/classes/portal.properties file.

b. Open the portal.properties file with a text editor.

c. Add the following line:

```
auth.pipeline.pre=com.dorado.nva.auth.CustomRadiusAuthenticator
```

This property causes the OMNM application to authenticate against the radius server prior to logging in through OMNM authentication. To skip OMNM authentication, continue with step 3. Otherwise, continue with step 4.

3 Edit the server-overrides.properties file if you only want to authenticate against the radius server.

a. Navigate to the *installDir*/oware/synergy/conf/server-overrides.properties.sample file.

b. Rename the server-overrides.properties.sample file to server-overrides.properties.

c. Open the server-overrides.properties file with a text editor.

d. Add the following line:

```
auth.pipeline.enable.liferay.check=false
```

If this line is set to false, the OMNM system authenticates against the radius server only. If set to true (or not set), authentication must pass at both the radius server and local OMNM authentication.

4 Verify that authentication work as defined.

Configuring Pages and User Access

This section describes adding pages to your OpenManage Network Manager (OMNM) installation, and configuring role-based user views. This is a way to manage user access to the OMNM features in a more complex environment. Configuring pages and user access involves:

- Creating Users
- Creating and Rearranging Pages
- Setting Page-Level Permissions
- Setting Portlet-Level Permissions
- Setting Resource-Level Permissions

Pages display portlets in the following ways:

Display Mode	Description
Summary/ Minimized Mode	Any portlet's that have the *Settings* toolbar option (Filters and Max Results) can save/toggle the Current Filter, Max Results, Max Items Per Page, and column choices. See Portlet Tools and Options on page 448. **Note:** The Max Results settings for summary portlets differ from those for maximized/expanded portlets. If you are an Admin and are on the Main portal site, OpenManage Network Manager saves these permanently. If you are a REGULAR user they are only saved temporarily unless the portlet is on your personal Public/Private pages. See Public/Private Page Behavior on page 676 for details.

Display Mode	Description
Maximized/ Expanded Mode	The *Settings* button in expanded portlets lets you configure displayed columns and their order, and the number of items to display. If the number of items in a list exceeds the maximum specified, a *[limit reached]* message appears next to the number of items listed in the bottom right corner of the page. **Note:** For large list, filters are a more efficient use of computing resources than large maximum settings. See Defining Advanced Filters on page 86 for more about configuring filters.

Creating Users

Create users as follows.

1 Go to the Control Panel.

2 Under the Portal category, click *Users and Organizations*, then click the *Add* > *User* menu item.

3 Fill out the User form with name and email address and so on.

4 Click Save when finished.

The save was successful message appears.

NOTE:

The expanded form lets you fill out more information about the user.

5 Select the Password, enter a password for the user, and then click *Save*.

6 Click the *Roles* link.

A screen appears showing the roles to which your ID is currently assigned. By default, all users are assigned the Power User role, and to the User role.

7 Optionally remove the default PowerUser role, add the appropriate new role for the user with the +*Select* link, and then click *Save*.

You can optionally fill out other details later.

(You may want to do this step after configuring roles. See Adding and Configuring User Roles/ Permissions on page 34.)

8 Select Redcell > Permission Manager.

9 Remove any permissions from the User role you do not want the user to have.

Creating and Rearranging Pages

Create and rearrange pages as follows.

1 Sign in as an administration user.

2 Click *Add* > *Page* from the portal.

A field appears.

3 Enter the page name.

That creates a page with a blank title in the doc.

4 Click on that tab page to see it.

5 Click *Manage* > *Page*.

An editor appears that lets you configure the page, add child pages, and so on.

6 Re-arrange the portal pages from the tree on the left.

7 Click *Save* when configured as needed and then click the X in the upper right corner of this editor.

Your page should appear in the portal after you refresh it.

8 Click the page label to open any new page, and click *Add* > *Applications* to add portlets to that page.

You can also drag and drop the portlets within the page to rearrange them. The applications under the *Portal* node are open source, and not documented here. The rest are OpenManage Network Manager-connected, and are documented in this guide.

NOTICE

Use the *Search Applications* field at the top of the *Add* > *Applications* menu to find portlets nested within that menu's categories. The *Portal Applications* and *Global* categories includes generic portlets; the remaining categories are for OpenManage Network Manager portlets.

Setting Page-Level Permissions

Setting page-level permissions provide a user/group/role/organization access to a defined OMNM page. Set page-level permissions as follows.

1 Sign in as an administration user.

2 Click *Manage* > *Page*.

3 Expand the Page Layout tree.

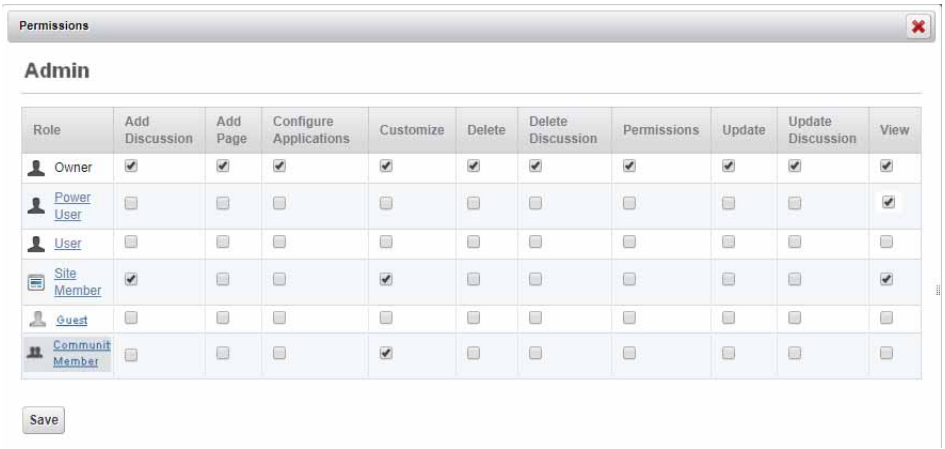
This represents the page layout as seen in the portal.

4 Select a page where you want to restrict access.

5 Click the *Permissions* button.

6 Deselect the *View* permission for Guest and Community members.

7 Make sure Owner and PowerUser can still view the page.



8 Now select *View* for any other roles you want to give access.

9 Click *Save*.

10 Verify that the user cannot see restricted pages by logging out and then logging in as the new user.

Setting Portlet-Level Permissions

The portlet-level permissions provide a user/group/role/organization access to a defined portlet. Configure portlet-level permissions as follows.

1 Sign in as an administration user.

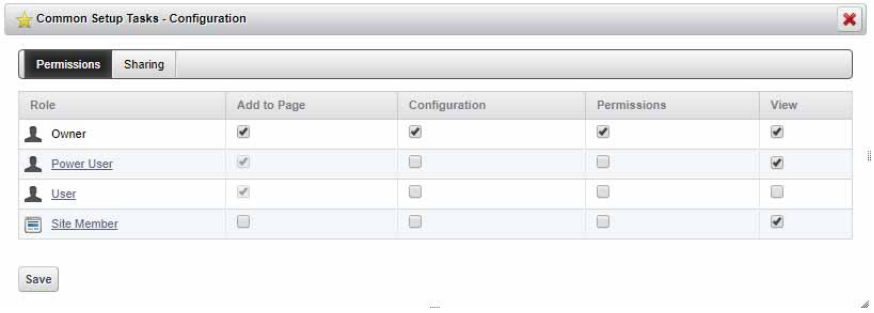
2 Click the Configuration tool (wrench) > Configuration for the appropriate portlet.



The Managed Resources - Configuration displays a list of permissions.

3 Deselect View permission for Guest and Community members.

4 Make sure Owner and PowerUser still have View permissions.



5 Select View for the relevant roles (for example, Silver Group).

6 Click Save.

7 Verify your configuration by logging out and then log in as Guest or another community member.

Setting Resource-Level Permissions

The resource-level permissions provide a user/group/role/organization access to a defined resource. Configure resource-level permissions as follows.

1 Create a Container for each Customer from the Container Manager portlet.

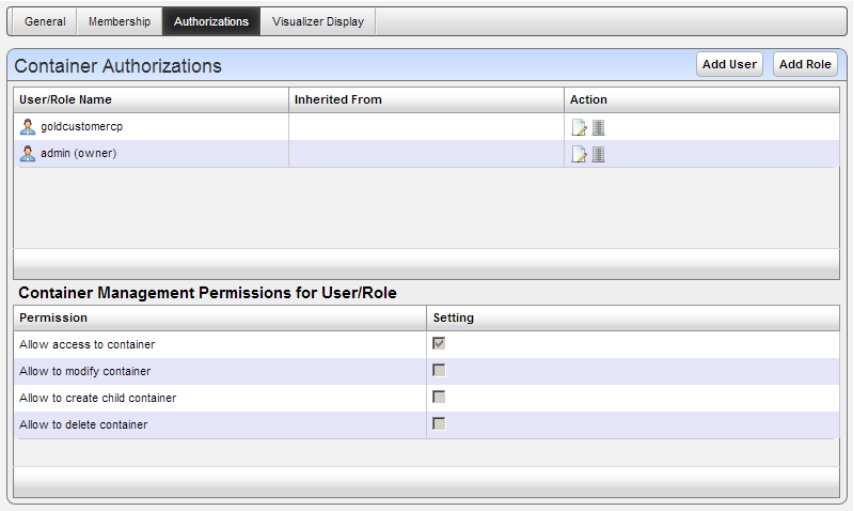
a. Right-click to select New.

The Creating New Root Container window is displayed.

b. Create a container for the desired Customer, naming and describing it.

c. Click Authorizations tab.

d. Add authorization for admin and select limited authorization for the desired customer (goldcustomercp, for example).



2 Configure the container's membership by selecting and adding a group of devices.

3 Set up a page for Device Level View.

a. Add a Container View to the page of interest with portlets for which you want to restrict access.

Currently Container View is enabled for the Managed Resources, Alarms, Ports, and Audit Trails portlets.

b. Log out as admin and then log back in as a user with Gold Customer permissions.

c. Confirm your permission configuration is operating on this page.

NOTICE

If you add sub-containers, the admin and goldcustomercp permissions "trickle down," so that users see the lower containers' contents. If you added, for example, silvercustomercp customer, that customer does not see the parent Gold container.

Registering a License

When it is time to register a license, you have the option to register the license using the OpenManage Network Manager (OMNM) application or using a command line interface.

Using the OMNM Application

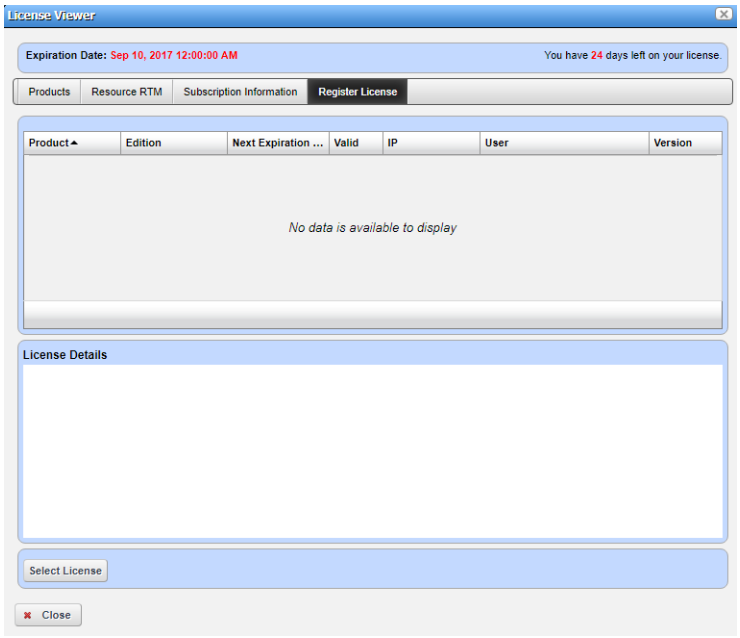
Register a license from the OMNM application as follows.

1 Select Settings > Application Configuration Settings > License Management option.

The License Viewer is displayed.

2 Click the Register License tab.

A blank license list is displayed.



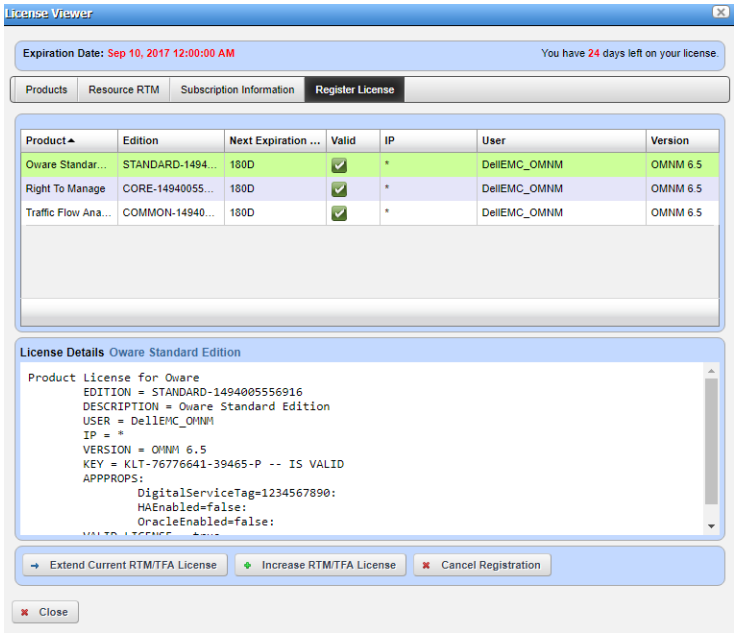
3 Click Select License.

4 Navigate to the license file, for example:

`license6.5_2000dd_180D_200tfa_ServiceTag_byGen.xml`

5 Select the file and then click Open.

The license information is displayed in the register license list.



6 Click one of the following registration types:

- Extend Current RTM/TFA License
- Increase RTM/TFA License

  See Register License on page 660 for more details about these options.

The license is registered.

7 Verify that the license was activated.

a. Click the Products tab.

b. Select the Oware product.

c. Look at the ACTIVATION DATE.

If you selected Increase RTM/TFA License, the activation date is today's date. If you selected Extend Current RTM//TFA License is the day the current license expires.

Using a Command Line Interface

Register a license from a command line interface (CLI) following the instructions for the appropriate operating system:

- Registering a License from Windows CLI
- Registering a License from Linux CLI

Registering a License from Windows CLI

1 Start the command line tool.

2 Enter `oware`.

3 Navigate to the *licenseFilename*.xml file.

4 Enter the following command:

`licenseimporter licenseFilename.xml`

If you want to specify an activation date, enter the following command using the activation option (-a*YYY-MMM-DD*):

`licenseimporter /aYYYY-MM-DD licenseFilename.xml`

Registering a License from Linux CLI

1. Start the command line tool.
2. Enter `. /etc/.dsienv`
3. Navigate to the *licenseFilename*.xml file.
4. Enter the following command:

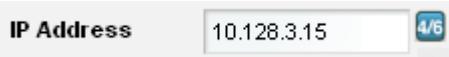
   `licenseimporter licenseFilename.xml`

   If you want to specify an activation date, enter the following command using the activation option (-a*YYY-MMM-DD*):

   `licenseimporter -aYYYY-MM-DD licenseFilename.xml`

Creating an IPv6 Discovery Profile

The OpenManage Network Manager (OMNM) system functions independently of the underlying IP protocol communication, so you can expect the OMNM application behavior to be the same regardless of whether resource management is through IPv4 or IPv6.



The following conditions indicate how to use such IP addresses in OpenManage Network Manager:

- When the blue *4/6* icon appears to the right of the IP address field means both IPv4 and IPv6 addresses are acceptable. When no icon appears, then only IPv4 addresses work.
- When a blue *6* icon appears, then only IPv6 addresses work. Notice that IPv6 does not support capital letters; lower case only.
- If a field supports IPV4/V6 and you enter something like `::ffff:192.2.2.2` then OpenManage Network Manager converts it to a standard address format after you tab off the field, perhaps adding some zeroes you did not enter.

IP v6 support exists for the following:

- Discovery—IPv6 Discovery profiles support single IPv6 entries, not IPv6 ranges and subnets. OpenManage Network Manager discovers devices configured to have an IPv6 management interface. If you discover a device with an IPv6 management interface, the discovery data collected on its ports and interfaces defaults to IPV4 if both IPv6 and IPv4 are configured on the same port or interface.

NOTE:

The ability to exclude a specific IP address on discovery profiles is limited to IPv4 only. IPv6 discovery at this time does not support ranges or subnets so exclusion is not necessary.

- Filters/Filtering/Target selection by IP address
- Editing the device management interface for IPv4 or IPv6
- Network tool portlet includes support IPv4 and IPv6

- Alarms, inventory reports, and other screens support IPv6 too.

CAUTION:
If you have a distributed installation, inter-server communication must be IPv4. **Also:** IPv6 is enabled by default. Add the following property to the owareapps/installprops/install.properties file to disable IPv6:

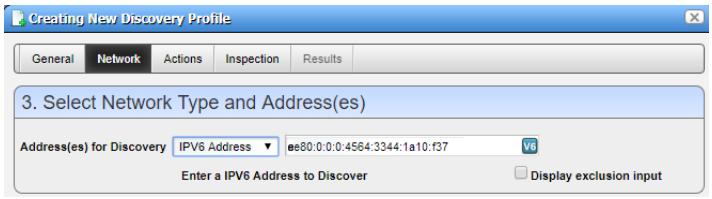
```
discovery.supports.ipv6=false
```

The following features are not supported:

- You cannot install to an IPv6 server.
- Distributed installations must communicate with IPv4

Create an IPv6 discovery profile as follows.

1. Create and name a Discovery Profile (see Discovering Your Network on page 59 for a more complete description).
2. Enter the IPv6 address in the second screen of a discovery profile in the editor.



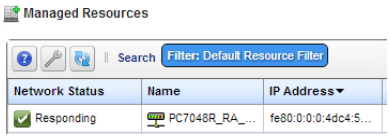
   Notice that an address like `de80::4564:3344:1a10:f37` becomes `de80:0:0:04564:3344:1a10:f37`, inserting zeros, when you tab off the address field.

3. Configure the discovery as you would like, and inspect to validate the device is ready to discover.

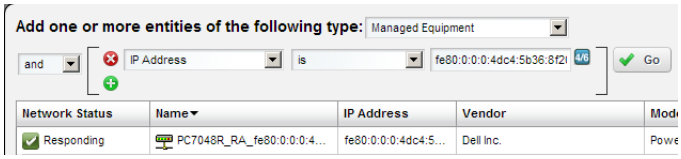
   Notice that if your network has switches without IPv6 enabled between your OpenManage Network Manager installation and the device you are discovering, inspection fails.

4. Execute discovery.

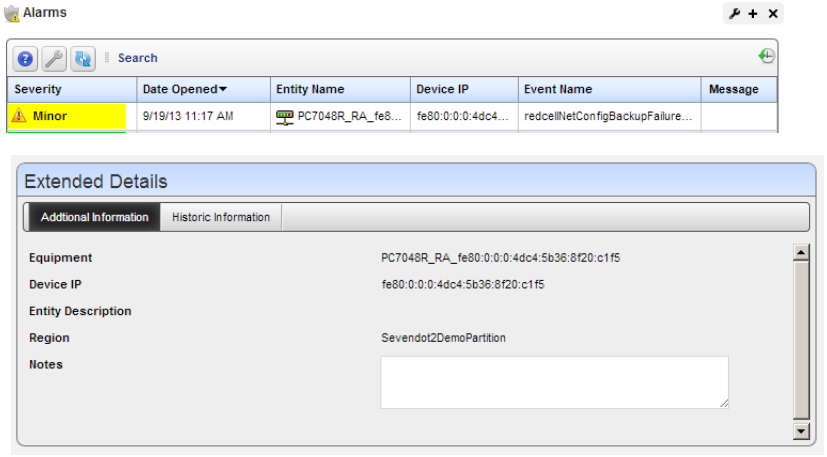
   The device appears in Managed Resources with the IPv6 interface in its IP Address column.



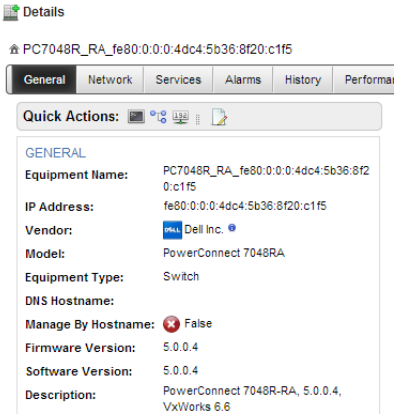
   It also appears in filters (like selecting device targets)



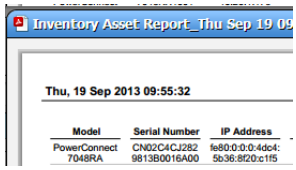
...and in various Alarm screens



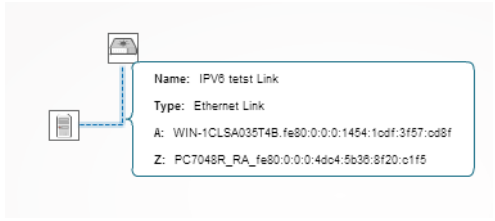
...and in Details panels



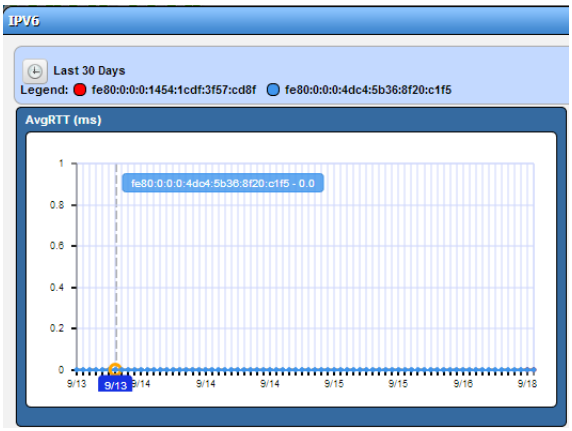
...and in Reports...



...and Visualize topologies

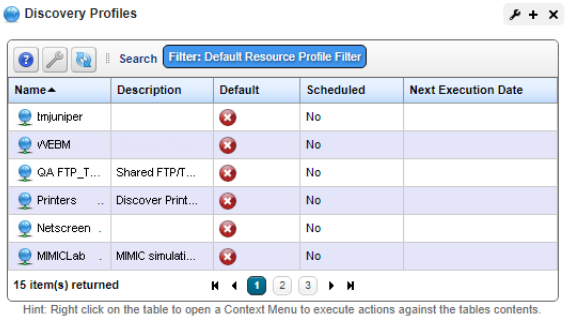


...and Performance Dashboards



Discovering Resources

Discovery profiles configure equipment discovery for OpenManage Network Manager.



The summary view displays the *Name*, *Description*, *Default* (the green check indicates the default profile), whether the profile is *Scheduled* and *Next Execution Date* for scheduled discovery.

The Expanded portlet adds a Reference Tree snap panel that displays a tree of associations between selected profiles and authentication and tasks that they execute. See Discovery Profiles Portlet on page 552 for more about this portlet.

You can import discovery profiles to target multitenant domains with a command line importer. The command is `importprofiles` and is in the `owareapps/redcell/bin directory.` This command takes the import file name an argument. The required domains should be available in the OpenManage Network Manager system before import occurs. Before importing discovery profiles to domains, any referenced authentications should be available in the domains or should be imported first by using the `importauths` command (the same way you would import discovery files). In other words, you should either manually create authentications for domains or import

authentication files using importauths command before importing discovery files to those domains. Example XML files (with the `<customer>` tag for domains) are in `owareapps\redcell\db`.

NOTICE

The date format follows the operating system's conventions for the location and language selected. Restarting the system changes system menus to the new language. If you want to revert back to the original language in Linux, you may also need to update the cache file under `/var/cache/gdm`.

The following tasks are related to discovering resources:

- Tuning Discovery Ping
- Discovering Your Network
- Determining Incomplete Discovery
- Configuring Resync
- Enabling Zero-Touch Provisioning and Auto-Discovery

Tuning Discovery Ping

During discovery, OpenManage Network Manager pings the devices specified in profiles. You can alter the defaults with the following properties:

```
redcell.discovery.timeout
redcell.discovery.retries
redcell.discovery.defaultport
```

Add these to the `owareapps/installprops/lib/installed.properties` file with the values you want preceded by an equal sign (=).

Discovering Your Network

The following steps describe how to discover devices on your network. You can also edit any seeded authentications and discovery profiles to see what they look like.

1 Right click the Discovery Profiles list and select *New*.

In a multitenant environment, you can create profiles exclusively for specific tenant sites (and the master site). A selector appears with a list of available sites if you have other sites configured.

2 The Discovery Profile Editor appears, with a step-by-step set of screens to configure resource discovery. You can navigate through it by clicking the screen tab names at the top, or by clicking the *Next* button at the bottom of the page.

This editor appears with the following panels:

General

3 **General Parameters**—Configure the *Name*, *Description* and whether this profile is the baseline default. Baseline discovery finds the baseline configuration to compare to later discoveries.

4 **Profile Options**—Select the *Device Naming Format* (how the device appears in resource lists, once discovered), whether to *Manage by* IP address or hostname, and check whether to *Resolve Hostnames*, *ICMP Ping Devices*, *Manage ICMP-only Devices*, or *Manage Unclassified*

Devices. This last option determines whether OpenManage Network Manager attempts to manage devices that have no device driver installed. Management may be possible, but more limited than for devices with drivers installed, provided this capability is one you have licensed.

NOTE:

Some packages disable ICMP ping by default.

The Filters (by *Location*, *Vendor*, or *Device Type*) let you narrow the list of devices discovered by the new profile. As the screen says, this filtering will not have any impact on the processing that occurs during the Inspection step.

Make sure you *Save* profiles you alter, or these selections have no impact when you execute discovery.

Network

5 After you click *Next*, the *Network* screen appears.

Network Type and Addresses—Select the type of entry in the pick list (*IP Address(es)*, *IP v6 Address*, *CIDR Address*, *Hostname*, *Subnet*).

NOTICE

You can specify an IP v4 Address range by separating the beginning and end with a dash. For example: 192.168.1.1-192.168.1.240.

Hover your cursor over the data entry field and the tooltips describe what valid entries look like.

You can exclude IP addresses, or ranges of IP addresses if you check the *Display exclusion input* checkbox and input the addresses you want excluded as you did for those you entered in the *Address(es) for Discovery* field. Such exclusions only apply to the profile where you enter them. To exclude an address or range, use the `com.dorado.redcell.discovery.exclude` property. Examples of how to enter such exclusions appear in the `redcell.properties` file under `owareapps\redcell\lib`. As always, best practice, if you want such properties to persist is to put the property in `owareapps\installprops\lib\installed.properties`.

6 **Authentication**—You can *Create new*, or *Choose existing* authentications. (See Authentications Portlet on page 628 for more about creating authentications.) Notice that authentications appear with *Edit*/*Delete* icons and *Up*/*Down* arrows on their right. The *Up*/*Down* arrows order authentications, so OpenManage Network Manager tries the top authentication first, then the next, and so on.

If you have an authentication like `admin/abc123` and one that is identical with an enable-level login/password (`admin/abc123/enable/enable123`), make sure the authentication with `enable` appears first in the list, otherwise, discovery finds the device, but does not access its enable functionality.

CAUTION:

If you do not get to the correct level of authentications—for example the "enable" user—then OpenManage Network Manager's full functionality is not available. The functionality will not be available for backup, restore, deploy, seeded or created actions that require a device enable login, Proscan, some performance monitoring that requires for OMNM to log into the device to retrieve an information using

command line interface (CLI). Also, some device information will be missing like firmware versioning, serial number, or port attributes when OMNM cannot retrieve that information using SNMP and needs to use CLI to retrieve that kind of information

NOTE:

Best practice is to avoid special characters, particularly # and > (command line prompts) in device banners so terminal access is unambiguous.

The *Edit* icon opens the authentication editor. Click the arrows to arrange the order in which the software tries credentials (top first). Ordering only applies when two credentials are of the same type.

Actions

7 You can configure Actions to run as part of discovery. By default, the actions screen includes the *Resync* action. For more about that, see Configuring Resync on page 62.

Use *Add Action* to select others to enter here. You can also edit parameters (if available), delete and re-order the actions listed here by clicking the icons to the right of them. OpenManage Network Manager executes them in top-to-bottom order.

By default discovery now automatically updates monitor targets with discovered equipment. For example, if you have a monitor targeting the dynamic All Dell Devices group, and discover a Dell device, discovery automatically adds the discovered device to the monitor's target list.

Device discovery initiated by web services does not require an existing discovery profile, however, if a default discovery profile exists, then discovery initiated by web services uses it. If you have updated your system, you must add the Refresh Monitor Targets action to any existing discovery profiles you have created before this default behavior occurs in upgraded discovery profiles.

You can change this default by changing the settings in the `/owareapps/redcell/lib/redcell.properties` file's `redcell.discovery.taskactivity.order` property. See also *Refresh Monitor Targets for Newly Discovered Devices on page 218*.

Inspection

8 **Inspect Network using your current settings**—This screen lets you preview the discovery profile's actions and access to devices. If you clicked *Next* rather than *Inspect* at the bottom of the previous screen, click *Start Inspection* to begin the inspection process for selected authentications that validates the device's credentials.

Notice that the *Inspection Status* fields below listed authentications indicates the success or failure of ping (if not disabled), Hostname resolution, and the listed Authentications.

If the device does not match all required authentications, you can click the *Fix it* icon (a wrench with a red or yellow dot) to edit them for the selected device. You can also click *Test Device*, *Create New,* or *Choose Existing* authentications while in the editor clicking the *Fix it* icon displays the authentication selection panel. The yellow dot on the *Fix it* icon means an optional authentication is missing. A red dot means a required one is missing.

When authentications are unsuccessful, you can remove or edit them in this editor too. Click the icons to the right of listed authentications to do this.

When they test successfully, the authentications appear in a nested tree under the *Discover* checkbox (checked when they test successfully).

9 **Save**—Click *Save* to preserve the profile. You can then right-click it to select *Execute* and begin discovery. If you select *Execute* from the profile editor, OpenManage Network Manager does not save the profile to execute later.

Results

10 **Execute**—Clicking *Execute* begins discovery, confirm you do not mind waiting, and the message traffic between OpenManage Network Manager and the device appears on the *Results* screen.

This is a standard *Audit* screen. See Audit Trail Portlet on page 630 for more about it. The Audit Trail portlet saves its contents if you want to see the message traffic between OpenManage Network Manager and the devices later.

11 A message (*Discovery Profile Execute is complete*) appears in the *Messages* at the bottom left of the status bar.

NOTICE

You can also schedule discovery profiles to run periodically, updating your database with any network changes. For more, see the options description in Schedule on page 671.

12 The devices in your network now appear in the Managed Resources portlet, and elsewhere (in the Network View topology, for example).

See Discovery Profiles Portlet on page 552 for more about these capabilities.

NOTE:

OpenManage Network Manager automatically adds discovered devices to the default ICMP monitor.

LLDP Warnings

Warning messages sometimes appear in the Discovery Audit Trail about LLDP. This occurs when the device's LLDP information indicates that a component exists with LLDP enabled at a certain IfIndex, but that IfIndex doesn't actually exist in the IfTable.

In other words, the information in the two SNMP tables does not match perfectly, OpenManage Network Manager warns about the IfIndexes that are missing. This incongruity in the tables is rather common and is not normally a problem, but OpenManage Network Manager still displays the warning.

The only time it would be of concern is if the warning claimed that it could not match IfIndex numbers that do exist in the IfTable, otherwise it's just a harmless warning that the LLDP table has some bad data in it.

Determining Incomplete Discovery

If the device is detected and responds to ping, but does not respond to actions (for example: Resync or Adaptive CLI), you may have only partially discovered it. Right-click the device in the Managed Resources portlet and select *Direct Access* > *Telnet*. If that menu option does not exist, the device is typically partially discovered with SNMP only. Right-click to edit the device, and add a both Telnet Management Interface and Authentication in those two tabs of the editor.

Configuring Resync

Resync now can retrieve, and if it is obsolete, update, the information gathered on initial discovery. Fields retrieved/updated include SysDescription, Contact, and Location.

OpenManage Network Manager can also retrieve the device's SysName to update the device's *Name* field on resync, depending on a system property. By default this is false, so no name retrieval occurs on resync.

The property determining this behavior is in `owareapps\ddbase\lib\ddbase.properties`. Here is how that property looks in `ddbase.properties`:

```
##Update Device Name on resync - 'false' turns this behavior off.
##Other options: sysname_ip , hostname_ip, sysname, hostname, and ip
##For example, to set this to use sysname + IP naming format, use
##com.dorado.devicedriver.base.updateName=sysname_ip
com.dorado.devicedriver.base.updateName=false
```

Best practice is to override the default in `owareappse\installprops\lib\installed.properties`.

△ CAUTION:

This property overrides the discovery profile's *Device Naming Format* convention selected. This can be useful if you want to force discovery to use a particular naming convention regardless of how others may have configured the Discovery Profile that initially retrieves information about the device discovered. It may be less-than-useful if a Resync action that follows or is part of the discovery process provides naming you do not want.

If you elect the default, resync still updates SysDescription, Contact and Location, but does *not* update SysName (*Name*).

If you have selected *Manage by Hostname* in your discovery profile, then resync will also retrieve any IP address changes, for example in a network with DHCP. Any override to resync's retrieved *Device Naming Format* may also change the device's *Name* when resync occurs if the IP address has changed, but it does not override the *Manage by Hostname* selection, and OpenManage Network Manager still keeps the originally retrieved hostname to refer to the device, even though it may not appear in the Managed Resources portlet and elsewhere.

Finally, you can manually override all retrieved *Name* information. Right-click a device and selecting *Edit*, then make the alterations. See Resource Editor: General on page 457. Such edits only alter OpenManage Network Manager's database, not data on the device. To alter data on the device, you can create an Adaptive CLI. See .

Resync overwrites any manual alterations if you make the resync property anything but the default.

Enabling Zero-Touch Provisioning and Auto-Discovery

Zero-touch provisioning is a process through which devices can be automatically configured and provisioned. Auto-discovery is a related process through which OpenManage Network Manager automatically discovers unmanaged devices that have been configured to send traps.

To **enable zero-touch provisioning** within your network, you need an external DHCP server. This server needs to be configured to automatically provision new devices with a basic configuration file. You can include any basic configuration settings you want within this file.

If you want to **enable auto-discovery**, then you need to configure the devices in your network to send traps to OpenManage Network Manager and you will also need to log into the OpenManage Network Manager web portal and follow a few configuration steps in order to activate this feature. Note if you want to use zero-touch provisioning in conjunction with auto-discovery, then your basic configuration file that is provisioned to the device will need to include a setting that tells the device to send traps to the OpenManage Network Manager server. However, auto-discovery can be used independently of zero-touch provisioning and vice-versa.

To activate auto-discovery of network devices within your OpenManage Network Manager system, follow these steps:

1 Log into the OpenManage Network Manager web portal.

2 Click on the Discover tab.

The Discovery Profiles portlet is displayed.

3 Find the Device Auto-Discovery entry.

This is the discovery profile that will be executed when a trap is received from an unmanaged device, but it needs to be configured properly first.

4 Right-click and then select Edit this entry.

You might want to change some of the settings on the General tab. See Discovery Profiles Portlet on page 552 for more information about this edit screen and the available options.

5 Click the Network tab.

Note that unlike the other discovery profiles, within this record, the IP Addresses field is intentionally left blank because the IP address of the target device will come from the source IP address of the trap that is received from the unmanaged device.

6 Configure the credentials within the devices that you wish to auto-discover.

If you are using zero-touch provisioning, then you could include authentication credentials in the basic configuration file that is provisioned to the device.

This discovery profile was created with placeholders for the authentication credentials, as seen in the "Select Authentication" list. You will need to remove these entries from the list and create new entries that match the authentication credentials that the device is configured with.

7 Save the discovery profile.

8 Enable the event processing rule that will execute this discovery profile so that it will be triggered when a trap is received from an unknown device.

9 Expand the Alarms menu item and click on Definitions and Rules.

The Automation and Event Processing Rules portlet is displayed.

10 Find the entry named "Execute Auto-Discovery when a trap is received from an unmanaged device".

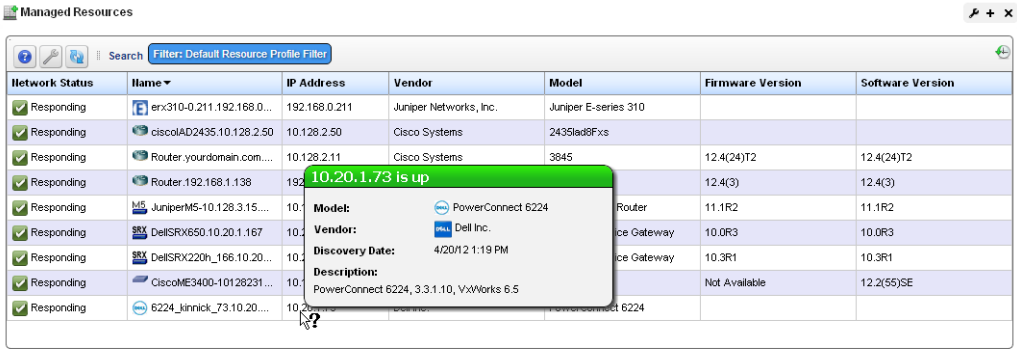
11 Right-click and then select Edit this entry.

Everything within this event processing rule should already be configured properly.

12 Select the Enabled option and then click Save.

Once the event processing rule is enabled it will be triggered any time a trap (or syslog) is received from an unmanaged device. If auto-discovery is used in conjunction with zero-touch provisioning, and if all the pieces are configured properly, then OpenManage Network Manager will automatically discover a device shortly after it has been provisioned by the DHCP server.

The Managed Resources portlet displays all discovered devices.



See Managed Resources on page 454 for the capabilities details and Managed Resource Groups Portlet on page 637 for the ways combine devices on which you can act.

Resetting a Password

You can reset a user's password two ways. One is to login as admin and change the user's password in Portal Settings > Users and Organizations. For additional information please refer to Portal > Users and Organizations on page 675.

For the second method, users themselves can request an email be sent to them with instructions to set a new password. Follow the steps below.

1 Login fails. At the bottom of the login screen is the Forgot Password link.

2 A prompt appears for user to enter a Screen Name.

3 A prompt appears to enter the answer to the reminder question (their Father's middle name) that they set when logging in the first time.

4 After entering the correct answer for their account, OpenManage Network Manager sends an email to the user's email address. E-mail for password reminders/resets requires setting up the fields in Control Panel > Server Administration > Mail, not the SMTP Configuration which is for OpenManage Network Manager-originated e-mails.

   After entering an incorrect answer, a request failed screen appears, with another chance for entering a correct answer.

5 The e-mail provides a link where the user can enter a new password and confirm it.

Deploying Add-On Capabilities

OpenManage Network Manager (OMNM) add-on capabilities come in the following forms:

- Deploy Updates
- Extensions
- .ocp and .ddp files

These add-on capabilities do not require a complete re-installation of the application. If you are upgrading to an entirely new OMNM package, refer to the *OpenManage Network Manager Installation Guide* for the upgrading from a previous version instructions. If you are updating your operating system, refer to the *OpenManage Network Manager Installation Guide* for instructions.

The following sections describe how to update your initial system with them.

Add-On Capability	Description
Deploy Updates	Updates to OpenManage Network Manager can come in .war files. For example, a new helpset (nvhelp.war), that updates the information about the program. To deploy such files, copy them to the *installDir*\oware\ synergy\deploy directory. A few minutes later, the OMNM application deploys them.
Extensions	Extended capabilities for the OMNM application may appear in .jar files. For example, the synergy-msp.jar file. To deploy these, copy the file into the *installDir*\oware\synergy\extensions directory.

.ocp and .ddp files	Device drivers and additional application capabilities come in files with the .ddp and .ocp extensions, respectively. These install automatically during the full OMNM installation when they are in the owareapps directory. To install them after your system is already up and running, use the following command line programs:
	`ocpinstall -x [filename.ddp or filename.ocp]`
	`ocpinstall -l [filename.ddp or filename.ocp]`
	`ocpinstall -s [filename.ddp or filename.ocp]`
	Note: You must install these to all application servers in a distributed environment.

Using Device Drivers

For complete communication with devices, the OpenManage Network Manager (OMNM) application requires a device driver. For example, to communicate with Dell EMC devices, you must have a Dell EMC driver installed. That does not mean you cannot discover and communicate with other vendors' devices without a driver installed. See .ocp and .ddp files on page 66 for driver installation instructions. The following sections include discussions of some of these drivers:

- Base Driver
- Supported PowerConnect Models
- Windows Management Instrumentation (WMI) Driver
- Web-Based Enterprise Management (WBEM) Driver

Base Driver

If you have no driver installed, the OpenManage Network Manager (OMNM) application provides the following functionality, depending on the devices' supporting and providing data from the SNMP system group (sysDescr, sysObjectID, sysUpTime, sysContact, sysName, sysLocation) and the ifTable, which provides list of device interface entries from the RFC1213-MIB. The OMNM application also depends on the entPhysicalTable in the ENTITY-MIB, which provides a list of physical entities contained on a device. If the device does not support the ENTITY-MIB, then the OMNM application bases sub-component creation entirely on ifTable contents.

Confirm that a device is not part of those supported by installed drivers when part of its OID is 3477.

Functionality	Description
Top Level Resource	The OMNM application creates top level resource for discovered devices with the following attributes: Equipment Name, Description, IP Address, Location, Contact, Vendor, Model, System Object Id, Date created, Creator, Discovery date, Last Modified.

Functionality	Description
Subcomponents	The OMNM application creates subcomponents (modules, ports, interfaces, power supplies, fans, and so on) for discovered device based on contents of entPhysicalTable.
Port/Interface Attributes	The OMNM application sets Port/Interface Attributes depending on port/interface type: Name, Port Description, MAC Address, Administrative State, Operational State, Port Type, Speed, Encapsulation, Operation Type, Switch Mode, CLI Name, If Index, Port Number, and Slot Number.
Direct Access	SNMP and Ping (ICMP) are enabled.
Monitors	The OMNM application automatically adds discovered device instances to the Default ICMP Monitor to indicate their Network Status. Support for SNMP based performance monitors using discovered ports and interfaces as targets is also possible. For example, Bandwidth Utilization.
Reports	You can execute reports like the Port Inventory Report or Device Inventory and results should include discovered device and device port entities.
Network View	Discovered devices and their sub-components appear, regardless of whether a device driver exists for them.
Events	The OMNM application supports standard MIB-II traps for discovered device and or sub-components. For example, linkUp, linkDown, coldStart, warmStart, and so on.
MIBs	The OMNM application can import MIBs for use within MIB Browser and performance monitoring so you can query device-specific OID values on discovered device.
Containers	Depending on the licensing, device and or contained sub-components are selectable and manageable in filters and portlets like Containers.
Links	You can manually create Links using discovered device or device subcomponents as end points which are then visible in Network View.
Attributes	You can manually populate or modify device/port attributes. For example Serial Number, Firmware Version, Port Type, Notes etc. Attribute values should then be included in reports based on a given report template.

Supported PowerConnect Models

Refer to release notes for a list of supported devices. From the OpenManage Network Manager (OMNM) application portal, select Manage > Show Versions to view information about supported devices and operating systems.

Windows Management Instrumentation (WMI) Driver

The Windows Management Instrumentation (WMI) driver currently supports any Windows-based operating system that supports the WMI. This driver must install supported versions of Windows. Refer to the *OpenManage Network Manager Installation Guide* for supported operating systems.

This driver supports global group operations. Discovery may display benign retry warning messages in the application server shell or log. You can safely ignore these.

Before installing the WMI driver, make sure that completed all prerequisites. Then, prevent WMI requests from being blocked by configuring the firewall.

Prerequisites

Before installing the OpenManage Network Manager (OMNM) application to manage other computers with a WMI driver, you must download and install the Microsoft .Net framework version 3.0 or later on the application server if it is not already installed there. For complete functionality, the WMI login for this software must be a login for a domain user who also belongs to the administrator group on the WMI device. Both are requirements for any installation managing WMI devices.

NOTICE

If you have complied with the prerequisites for installation and do not need the basic installation instructions that appear in the next section, refer to the more detailed installation instructions in the other manuals for information about how to install OpenManage Network Manager in more complex environments.

The following are common Windows prerequisites:

Credentials—Use administrative credentials to manage the computer system with WMI.

Firewall—Allow those WMI requests that you want to manage as some firewalls installed may block WMI requests. (See Configuring the Firewall.)

License—Make sure that you have the proper licenses installed to discover the devices you want. If you have a Dell-only license and are discovering a non-Dell device, discovery does not work. Or if you have a Dell license for desktop discovery only, you cannot discover a server.

See License Viewer on page 653 for more about licenses.

Configuring the Firewall

Configure the firewall between your server and the Internet as follows.

1. Deny all incoming traffic from the Internet to your server.
2. Permit incoming traffic from all clients to TCP port 135 (and UDP port 135, if necessary) on your server.
3. Open Port 445 (WMI).
4. Permit incoming traffic from all clients to the TCP ports (and UDP ports, if necessary) on your server in the Ports ranges specified.
5. Permit incoming traffic on all ports where the TCP connection was initiated by your server if you are using callbacks.

   WMI queries succeed only if you add the user account to a local admin group. Refer to the Microsoft knowledgebase articles for the way to do this. For example, Leverage Group Policies with WMI Filters.

   For user rights for WMI access, see: www.mcse.ms/archive68-2005541196.html

   See also: *Service overview and network port requirements for the Windows Server system* (support.microsoft.com/kb/832017/)

Web-Based Enterprise Management (WBEM) Driver

The Web-Based Enterprise Management driver currently supports operating systems supporting the Web-Based Enterprise Management interface (WBEM).

WBEM is always installed on the following operating systems versions, and later:

- Red Hat Linux and/or CentOS 6.2, 6.4
- VM Ware (ESX) with WBEM installed.

You can install Web-Based Enterprise Management on some other systems if they do not already use it, but monitored devices must have this installed.

NOTE:

To verify WBEM is running on your system, run the following command: `ps -e | grep cim`. You should see a process labelled `cimserver`.

The following topics are related to the WBEM driver:

- Installing WBEM on Red Hat
- WBEM Prerequisites
- Secure WBEM Access
- VMWare ESX and KVM Controller Support

Installing WBEM on Red Hat

You can download and install WBEM support for Red Hat Linux. For example, for Red Hat 6.2, a release for WBEM is `tog-pegasus-2.12.0-3.el6_4.x86_64.rpm`. This is what you need to download once you have logged into the Red Hat network.

Install this as follows:

Install: `rpm -ih tog-pegasus-2.12.0-3.el6_4.x86_64.rpm`

Upgrade: `rpm -Uh tog-pegasus-2.12.0-3.el6_4.x86_64.rpm`

To determine if wbem is running, run `ps -ef | grep cimserver` in a shell.

To start | stop | get status of the WBEM service:

```
tog-pegasus start | stop | status"
```

WBEM Prerequisites

The following are common prerequisites:

Credentials—WBEM credentials have a role in discovering the device. Your system must have access to the computer using Administrative only credentials. These are the same credentials as the user installing WBEM on the device.

Telnet/SSH credentials are necessary for other supported applications.

For full functionality, this WBEM device driver requires administrative (root) access. Many devices may only allow root logins on a local console.

In such cases, configure the Telnet/SSH authentication for these devices to login as a non-root user—and, in Authentication Manager, enter `su` in the *Enable User ID* field and enter the root user's password in *Enable User Password* in that same authentication. This enables full device management functionality with root access.

Credentials for Telnet/SSH should have a privilege level sufficient to stop services and to restart the computer system.

Firewall— Some firewalls installed on the computer may block WBEM requests. Permit access for those you want to manage.

License—Make sure you have the correct WBEM driver license installed. Licenses come in the following types:

- Major Vendor by Name - Such as Dell, Compaq, HP, Gateway.

- Server/Desktop individual license support.
- Generic computers - non-major vendors.
- ALL - this gives the driver all capabilities for any computer system.

NOTE:

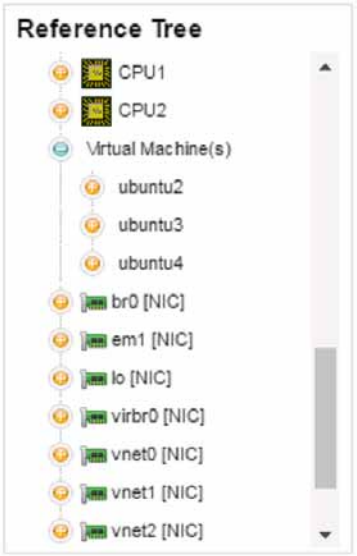
If you discover an Amigopod host that does not have its SNMP agent turned on, OpenManage Network Manager labels it a WMI or WBEM host rather than an Amigopod host.

Secure WBEM Access

Some monitoring capabilities require root access, even if you securely log into the Linux host. In this case, when configuring a secure (SSH) login, configure a telnet authentication with `su` as an *Enable User ID*, and the root user's password as the *Enable Password*. For other WBEM access, configure authentication as an HTTP/HTTPS login/password, and select WBEM as the protocol after you have selected the WBEM authentication.

VMWare ESX and KVM Controller Support

Basic support for management of VMWare ESX and KVM Controller devices has been added. The controllers are discovered/managed via WBEM protocol and require WBEM and SSH authentication protocol at discovery time. VMs will appear in the controller's reference tree, but can also be discovered standalone.



Example Reference tree for a KVM Controller showing three hosted VMs

Supported Functionality for VMWare ESX and KVM Controllers

VMWare ESX and KVM Controller devices support the following functionality:

- Discovery/Resync
- Limited KPI Support
- Direct Access/Terminal
- ACLI Support
- VM Management Actions

VM Management Actions

VMWare ESX and KVM Controller devices have specialized VM Management Actions that are available to them. These actions are accessible via the "Actions" menu that is available on a Managed Resource.

The following actions are supported for managing hosted VMS:

- Start
- Stop
- Suspend
- Resume
- Reboot

NOTE:

In order for some actions to function, the target hosted VM must be configured correctly. For VMWare ESX devices, please see: https://www.vmware.com/support/developer/vcli/ and ensure that the vSphere CLI tools are installed on the target guest VM. For KVM devices, please see: http://virt-tools.org/learning/start-stop-vm-with-command-line/, and ensure that the target guest VM is configured to respond to ACPI requests.

Optimizing Your System

This section provides the following tasks, which you can do to optimize your system:

- Overriding Properties
- Tuning Memory (Heap & Portal)
- Tuning Application Features' Performance Impact
- Resizing, Starting and Stopping MySQL

Overriding Properties

You can fine-tune various features of the application. Rather than lose those changes if and when you upgrade or patch, best practice is to override changes.

To do this for the Web portal, first rename the provided file `\oware\synergy\conf\server-overrides.properties.sample` to `server-overrides.properties`, and enable the properties within it by uncommenting them, and altering them to fit your needs. The comments in this file provide more information.

You can also override application server-related properties in

`\owareapps\installprops\lib\installed.properties.`

Both of these properties files remain as you previously configured them if you install an upgrade, but upgrades overwrite the `server-overrides.properties.sample`, so keep a copy if it has anything you want to preserve.

Screen names—One possible configuration property (`com.synergy.validation.screenmame.min.length`) specifies a minimum length for user screen names. For the existing user base then any screen names that are shorter than the value must change to the required length on the next edit/save for that user.

Tuning Memory (Heap & Portal)

You can adjust the memory footprint of any installed server's virtual machine (VM) by configuring it in the Heap configuration installation screen that appears during most package installations. Within limits, using more memory, if it is available, generally means better performance. Launching a server without sufficient memory produces the following error: `Error occurred during initialization of VM Could not reserve enough space for object heap.`

You can re-set these after installation too, with the following properties in `\owareapps\installprops\lib\installed.properties`:

```
oware.server.min.heap.size=3072m
oware.server.max.heap.size=3072m
```

For Windows and Linux valid settings range from 512m to the limit of available RAM minus operating system needs.

While you can enter any number within these constraints, the following are values that are supported during upgrade. Other values are ignored during upgrade and you must choose again from supported value list during installation/upgrade.

Portal Memory Settings

To manually change OpenManage Network Manager web portal heap settings, change the `setenv.sh` (Linux) or `setenv.bat` (Windows) file:

```
set "PORTAL_PERMGEN=512m"
set "PORTAL_MAX_MEM=3072m"
set "PORTAL_INIT_MEM=768m"
set "PORTAL_32BIT_MAX_MEM=768m"
```

These files are in the `Tomcat***/bin` directory. After you change their settings, for Linux, restart the portal service to apply new memory settings. In Windows, besides updating `setenv.bat` you must run `service.bat update` in that same directory.

You can increase these to even higher figures if your system has the memory available.

NOTICE

Make sure only one Tomcat process is running, otherwise your web server may exhibit poor performance.

Memory Limits Advice

RAM size on hardware can increase virtually without limit. However, if you configure application server so it does not use half of the configured Heap, then having such a large Heap degrades performance since Java (this software's programming language) scans and sizes garbage collection with the pre-allocated large Heap in mind.

That is not to say servers cannot have large amounts of memory. As the applications goes into production and usage grows, larger RAM lets you adjust to meet demand as it grows. Having a small amount of RAM does not allow for growth when needed.

Another thing to remember: Suppose a host has 32GB for an Application Server. Say the Application Server Heap is 28GB. This limits the amount of Threads you can run simultaneously in Thread Pools as well as I/O forking. Every time Java executes a thread, it allocates memory outside of its VM for native calls Since the server only had 32GB and the operating system must use some, very little remains for these processes.

Best practice: Lower the Heap Memory in favor or leaving some more available to the operating system so you can take advantage of more threads if you have the CPU cycles.

Too much Heap RAM impacts only excessive garbage collection which can equate to application pauses as garbage collection moves memory around. Application pauses degrade performance.

Tuning Application Features' Performance Impact

Resync, Performance, and so on use different pools than backups, so limiting the size of the backups pool would have little impact on resync since these applications does not compete for resources.

If you need to configure these, you can configure pool sizes using properties in `installed.properties`. On startup the application server creates a file called `mbean_attr_overrides.template` in `owareapps/installprops/lib`. This includes text descriptions of Mbeans and their setable properties. It allows you to copy properties you want to override and add them to the existing `install.properties`, so the settings persist even if you upgrade the software. This replaces a previous tuning method that required editing `mbean-settings.xml` and did not persist past upgrade.

For more about performance settings for monitors, see Best Practices: Performance and Monitors on page 157.

Authentication

For successful discovery of the resources on your network, OpenManage Network Manager requires authenticated management access to devices. To get such access, you must provide the correct SNMP community strings, WMI login credentials, and any other command-line (Telnet/SSH) or browser (HTTP/HTTPS) related authentication, and SNMP must active on devices, if that is not their default. Some devices require pre-configuration to recognize this management software. Consult your network administrator or device manuals for instructions about how to enable them and authorize OpenManage Network Manager as the management console. See Authentications Portlet on page 628 for more about authentication.

CAUTION:

If you do not get access to the deepest level of authentications—for example the "enable" user's—you cannot access all of OpenManage Network Manager's functionality.

Resizing, Starting and Stopping MySQL

MySQL Database Sizing—Installation includes the chance to select a size for your embedded database. This should reflect expected use, and should be small enough that you leave enough RAM for the application and operating system (at least 4G, typically).

NOTE:

The default MySQL login command line is: >mysql -u root --password=dorado

By default, installation optimizes the embedded database for the minimum hardware requirement. This may not be sufficient for some environments when your database size grows. You can set the database size during installation, and further tune performance parameters in following file:

`..oware3rd\mysql\[version number]\my.cnf`

Have your MySQL operational expert review the links cited below to determine the best values for your environment.

1 Set `innodb_buffer_pool_size=512m` to `16382m`.

Best practice is to make your buffer pool roughly 10% larger than the total size of Innodb TableSpaces. You can determine total tablespace size with the (free download) MySQL Workbench application.

If your database size is 30G, ideally have a buffer size of 33G or more. You can also investigate limiting database size or consider adding extra RAM. For dedicated database server, we recommend 70%-80% of system server's RAM, for example use 16G of RAM for a server with 24G RAM total.

To avoid operating system caching what is already cached by this buffer you may have to make additional adjustments. This is not necessary on Windows, but for Linux you need to set `innodb_flush_method=O_DIRECT`.

You may want to make MySQL to use Large Pages for allocating Innodb Buffer Pool and few other buffers. Tuning your VM to be less eager to swap things with `echo 0 > /proc/sys/vm/swappiness` is another helpful change though it does not always save you from swapping.

The optimal setting for Inno DB buffer is to have buffer pool hit rate of 1000/1000)

```
mysql> SHOW ENGINE INNODB STATUS\G
----------------------
BUFFER POOL AND MEMORY
----------------------
Buffer pool hit rate 1000 / 1000
```

You may need to modify system settings, increase or decrease application server heap, web server heap, and innodb buffer to fit your needs. This depends on whether you use the webserver heavily.

2 Set `innodb_log_file_size = 256 M` to `1024m`.

A larger file improves performance, but setting it too large will increase recovery time in case of a crash or power failure. Best practice is to experiment with various settings to determine what size is best for performance.

To change the log file size, you must move existing the log files named ib_logfile0, ib_logfile1, and so on. See Changing InnoDB Log Files in MySQL on page 76 for step-by-step instructions. The database may not start if you configure a log file size mismatch.

3 Set `max_connections=100` to `1000`.

Best practice is to configure 200 or more connections per server (application server + web server), especially if you are adding more servers.

The number of connections permitted in this version of MySQL defaults to 100. If you need to support more connections, set a larger value for this variable. Windows is limited to (open tables × 2 + open connections < 2048) because of the Posix compatibility layer used on that platform.

4 Log in to mySQL to check current settings:

```
mysql -u root --password=dorado
mysql> show variables like 'max_connections';
```

To check open connections:

```
mysql> SHOW STATUS WHERE `variable_name` = 'Threads_connected';
```

NOTE:

You may need to reduce `table_cache` if you increase `max_connection`.

5 `Set table_cache = 1024` (increase the default as appropriate).

`table_cache` is related to max_connections. For example, for 200 concurrent running connections, you should have a table cache size of at least 200 * N, where N is the maximum number of tables per join in any of the queries which you execute. You must also reserve some extra file descriptors for temporary tables and files.

If the value is very large or increases rapidly, even when you have not issued many FLUSH TABLES statements, you should increase the table cache size.

6 **Monitors:** If you enabled and configured the default SNMP interface monitor, it would typically consume most of the space in owbusdb (the database).

Unless you have reason to do otherwise, best practice is to disable *Retain polled data* on the default SNMP interface monitors. The graphs do not need these data for display. OpenManage Network Manager only uses retained data to derive the calculated metrics attributes. In most cases, saving only calculated data for the default SNMP interface monitor suffices.

For example, if you have 16 polled data attributes and 27 calculated attributes, not saving polled data can reduce the table size about 35%.

You can further reduce the table size if you only poll/save the relevant calculated attributes in the default SNMP interface monitor. To accomplish this you must remove calculated/polled attributes that you do not want to retain from the monitor configuration, OpenManage Network Manager does not support selectively choosing which attributes to keep. Retained attributes can be all calculated or no calculated.

NOTE:

Best practice is to archive the modified database sizing file somewhere safe. Upgrading or patching your installation may overwrite your settings, and you can simply copy the archived file to the correct location to recover any configuration you have made if that occurs.

If you want to change the size of your database after you have installed it, edit the `my.cnf` file in `/oware3rd/mysql/[version number]/`. Alter the last number on the following line:

```
[path]/oware3rd/mysql/ibdata/ibdata1:1024M:autoextend:max:102400M
```

To start MySQL, run the following in a shell:

```
[path]oware3rd/MySQL/[version number]/bin/mysqld" --console
```

When it starts successfully, the console includes a `ready for connections` message. Without the `--console` parameter, MySQL writes diagnostic output to the error log in its `data` directory.

To stop MySQL, run the following in a shell on the path with MySQL:

```
mysqladmin shutdown
```

Other operating system-specific shutdown initiation methods are possible as well: The server shuts down on Linux when it receives a SIGTERM signal. A server running as a service on Windows shuts down when you shut it down in Windows' services manager.

NOTE:

The default MySQL login command line is: >mysql -u root --password=dorado

Changing InnoDB Log Files in MySQL

To change the Number or Size of InnoDB redo log Files, follow these steps:

1 Set innodb_fast_shutdown to 1 if it is set to 2.

```
mysql> SET GLOBAL innodb_fast_shutdown = 1;
```

2 After ensuring that `innodb_fast_shutdown` is not set to 2, stop the MySQL server and make sure that it shuts down without errors (to ensure that there is no information for outstanding transactions in the log).

3 Copy the old log files into a safe place in case something went wrong during the shutdown and you need them to recover the tablespace.

4 Delete the old log files from the log file directory.

5 Edit `my.cnf` to change the log file configuration.

6 Start the MySQL server again. mysqld sees that no InnoDB log files exist at startup and creates new ones.

SNMP in Multi-Homed Environment

Trap listener, Inform listener and all outbound SNMP requests must bind to a specific interface in a multi-homed environment. This interface is considered appropriate to use for all network-facing SNMP activity. By default, this is `localhost`, interpreted as the application's local IP value (the NIC selected at installation time). The following text in `installed.properties` provides a specific IP address to control outbound SNMP interface binding on the local machine:

```
# specific interface used for all NMS initated
# communications to the network
com.dorado.mediation.outbound.address=localhost
```

Include the following and provide a specific IP address to control inbound (listener) interface binding on the local machine:

```
#
# specific interface used for binding mediation
# listeners such as SNMP trap listener
com.dorado.mediation.listener.address=localhost
```

Events with no corresponding definition appear as alarms of indeterminate severity. The only way to change behavior of an unknown event in this version would be to locate the missing MIB and load it into the system. This creates the missing event definitions needed to specify explicit behaviors.

Maintaining and Repairing Your System

The following describes ongoing tasks that keep your OpenManage Network Manager system functioning without interruptions. Some of these take advantage of pre-seeded features, and others take manual intervention.

- Troubleshooting a Balky Application
- Revising Database Aging Policies (DAP)
- Reviewing Scheduled Items
- Backing Up and Administering the Database
- Cleaning Up Logs
- Cleaning Up Files

Troubleshooting a Balky Application

Suggested mini-troubleshooting steps for a balky application that is already installed and running:

1 Refresh the browser.

If that does not work continue.

2 Clear the browser's cache (Firefox in particular loves persistent old pages), then refresh.

If that does not work continue.

3 Stop and start the browser.

If that does not work continue.

4 Stop and start the Web server

For Windows, to start the web server manager:

`oware\synergy\tomcat-X.X.X\bin\startsynergy.`
For Linux.

`/etc/init.d/synergy start` or `/etc/init.d/synergy stop`
Worth noting: The tray icon for the web server () is "optimistic" about both when the web server has completely started and completely stopped. You cannot re-start web server when its Tomcat process still lingers. If you lack patience, kill the (large) Tomcat process then re-start web server. The smaller one is that tray icon.

If that does not work continue.

5 Stop and start application server.

Command lines for this:

`stopappserver and startappserver`
If that does not work continue.

6 Delete the contents of the `oware/temp` directory and restart application server.

If that does not work continue.

7 Reboot the host and re-start the application server, web server and browser.

When troubleshooting (or contacting technical support), you may find pertinent information in logs located in the following directories:

```
..\oware\jboss-3.0.8\server\oware\log
..\oware\temp\soniqmq.log
..\app_setup.log
..\db_setup.log
```

Best practice is to run the getlogs script from a command line. It packages relevant logs in a logs.jar file in the root installation directory, and moves any existing copy of the logs.jar file to oware\temp. The logs.jar file compresses all logs necessary for troubleshooting. Read the jar yourself, or forward this jar to technical support for help in troubleshooting.

Searching \oware\jboss-5.1\server\oware\log\server.log for "error" is one way to look for the root of application server problems.

NOTE:

If you see errors that say your Linux system has too few threads, make sure that you have set the file handles correctly.

Revising Database Aging Policies (DAP)

DAP policies automatically purge or archive stale data so the database can maintain its capacity. Several pre-defined and pre-seeded DAPs come with OpenManage Network Manager. You may need to revise these to fit your system. These start at specific times—see the Schedules portlet for specifics about when.

DAPs amount to preventative maintenance since they help to maintain the database's capacity. Best practice is to do the following regularly:

1. In the Audit Trail Manager, create a Filter for Creation Date = prior Month and Action = DAP Executed.
2. Review the records for Status – Failed. These indicate that a DAP job failed. As long as the following DAP jobs execute, no immediate action is required. If any DAPs are repeatedly failing, then consult the troubleshooting document or OpenManage Network Manager support.
3. Review the DAP jobs entries and compare to the scheduled DAP start times. Confirm that audit records are displaying a corresponding audit record for each scheduled execution.

Reviewing Scheduled Items

Reviewing schedules to ensure that scheduled task are executing as expected.

1. In the Audit Trail portlet, create a Filter for each scheduled action and confirm that the schedule action is successful. The schedule "Type" is the Audit Filter Action.
2. Investigate any failure of a scheduled action.

Backing Up and Administering the Database

Backup your database regularly. Best practice is for the Oracle database administrator is to perform a monthly Full backup with Daily incremental backups. Best practice is for the Database Administrator to check monthly to ensure that the application has sufficient resources. See Backing Up the Database on page 39 and Restoring Databases on page 40.

Cleaning Up Logs

The `server.log` files may accumulate over time. Best practice is to purge these once a month. The server.log files are in the directory `<installation root>\oware\jboss-5.1\server\oware\log`. Archived these if you need historical log data. Best practice is to store only a maximum of 30 days worth of log files.

Installation Logs may also accumulate in `<installation root>\logs`. Best practice is to review this directory monthly and purge it as needed. Best practice is to retain at least 6 months to a year of log data in this directory.

Cleaning Up Files

When you turn on CLI trace, this software generates a log file for every CLI transaction and stores them in the `oware\temp` directory. This directory may accumulate many files if you leave CLI trace on for an extended period. You can delete or archive these files. Best practice is to inspect the directory and take the appropriate action at least once per month.

When backing up/ restoring configuration files or deploying OS images using the internal file server, a copy of the file may remain in `oware/temp`. You can delete the contents of this directory since it is auto created.

External file servers used in the production environment may also accumulate a copies of transferred files. Best practice is to review space on these file servers monthly to ensure the file server space is adequate.

2

Configuring the Portal

The following explains how to customize the OpenManage Network Manager (OMNM) portal. Because this portal can be so flexible, and comes from open source features, this is not a comprehensive catalog of all its features. The following discussion covers only those features significant for using the OMNM application.

Setting Time Formats – 82
Defining a Custom Debug – 82
Activating Log4J Email Feature – 82
Hiding Portlet Hint Text – 85
Modifying Column Settings – 85
Defining Advanced Filters – 86
Exporting/Importing Page Configurations – 87
Sharing a Resource – 87
Editing Custom Attributes – 88
Configuring Job Viewer's Appearance – 89
Scheduling Actions – 90

Setting Time Formats

To set the time display in various locations (alarms, schedules, and so on), set the operating system's time format as you would like. These example steps show how to set the Australian default day, month, year for the Windows 10 operating system.

Set Windows time formats as follows.

1. Navigate to the Control Panel.
2. Select Clock, Language and Region.
3. Click Change Date, Time, or number formats.

   The Region window displays the format settings.
4. Verify that the format is: English (Australia).
5. Click the Administrative tab.
6. Click on Copy settings.
7. Select both these options:
   - Welcome screen and system accounts
   - New user accounts
8. Click OK.
9. Restart the application server.
10. Verify that the Day/Month format appears in your portlets.

Defining a Custom Debug

For more advanced users, any component under owareapps can define a log4j.xml debug file for each component matching the following pattern:

```
owareapps\<component-dir>\server\conf\*log4j.xml
```

Consult these files for categories you want to change, and copy those altered properties to the file you created in the owareapps\installprops directory. The categories altered in this file override any others. Changing such properties can produce enhanced error output in server logs. See also Application Server Statistics on page 167.

Activating Log4J Email Feature

The activation steps vary depending on whether you are activating the log4j email feature on the application/mediation server or on the Web server.

Defining Log4J on Application or Mediation Servers

The application and mediation servers use JBoss, which defines Log4J settings through XML. Define the log4j email feature on Application or Mediation servers as follows.

1. Go to the .../oware/conf/ directory
2. Find the server-log4j.xml file.
3. Add the following alongside the other <appender> tags:

```
<!-- If this is present the processing of SMTP will be asynchronous.  It is
    not required -->
  <appender name="ASYNC" class="org.apache.log4j.AsyncAppender">
    <errorHandler class="org.jboss.logging.util.OnlyOnceErrorHandler"/>
    <appender-ref ref="SMTP"/>
  </appender>

  <!-- These are the main settings.  Note that "SMTP" here is just a name.
    You choose any name you want
       and in fact you can have more than email appender -->
  <appender name="SMTP" class="org.apache.log4j.net.SMTPAppender">
<errorHandler class="org.jboss.logging.util.OnlyOnceErrorHandler"/>
    <param name="Threshold" value="ERROR"/>
    <param name="To" value="destination@email"/>
    <param name="From" value="sender@email"/>
    <param name="Subject" value="Testing Log4J Email feature"/>
    <param name="SMTPHost" value="email.com.au"/>
<!-- you might need this <param name="TLS" value="true"/> -->
    <param name="SMTPUsername" value="myusername"/>
    <param name="SMTPPassword" value="mypassword"/> -->
   <param name="BufferSize" value="10"/> <-- find an appropriate value for
   this -->
    <layout class="org.apache.log4j.PatternLayout">
      <param name="ConversionPattern" value="%m"/>  <!-- read more at
   https://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/
   PatternLayout.html -->
    </layout>
  </appender>
```

4. Find the server-log4j-tail.xml file.
5. Change the file to something like this:

```
<root>
      <appender-ref ref="CONSOLE"/>
      <appender-ref ref="FILE"/>
      <appender-ref ref="SMTP"/>
</root>
```

6. Restart the server.

Defining Log4J on Web Servers

Web servers use Tomcat, which defines Log4J settings through a properties file. Define the log4j email feature on Web servers as follows.

1 Go to the following directory:

```
.../oware/synergy/tomcat-7.0.40/webapps/netview/WEB-INF/classes
```

2 Find the log4j.properties file.

3 Change the file to something like the following example, as appropriate.

You may want to use some of the same values from the XML file used for the application server.

```
log4j.logger.com.dorado=INFO, CONSOLE
log4j.logger.com.dorado.netview.social=DEBUG, CONSOLE
log4j.logger.com.icesoft=WARN, CONSOLE
log4j.logger.com.icesoft.faces.async.render=TRACE, CONSOLE

log4j.appender.CONSOLE=org.apache.log4j.ConsoleAppender
log4j.appender.CONSOLE.layout=org.apache.log4j.PatternLayout
log4j.appender.CONSOLE.layout.ConversionPattern=%d{ABSOLUTE} %-5p
    [%c{1}:%L] %m%n
log4j.rootLogger=ERROR, EmailAlertsAppender
log4j.appender.EmailAlertsAppender=org.apache.log4j.net.SMTPAppender
log4j.appender.EmailAlertsAppender.From=sender@email
log4j.appender.EmailAlertsAppender.To=destination@email
log4j.appender.EmailAlertsAppender.Threshold=ERROR
log4j.appender.EmailAlertsAppender.SMTPUsername=myusername
log4j.appender.EmailAlertsAppender.SMTPPassword=mypassword
log4j.appender.EmailAlertsAppender.SMTPHost=email.com.au
log4j.appender.EmailAlertsAppender.BufferSize=10
log4j.appender.EmailAlertsAppender.Subject=Testing Log4J Email feature
log4j.appender.EmailAlertsAppender.layout=org.apache.log4j.PatternLayout
log4j.appender.EmailAlertsAppender.layout.ConversionPattern=%m
log4j.appender.EmailAlertsAppender.EvaluatorClass=TriggerLogEvent
log4j.appender.EmailAlertsAppender.TLS=true
```

4 Restart the Web server

NOTE:

Your settings are overwritten on upgrade. Make sure that you backup the appropriate files before upgrading and then restore the files after upgrading.

Hiding Portlet Hint Text

By default, all portlets display hint text at the bottom. Hide the portlet hint text as follows.

1 Stop the Web server.

For example, enter the following from the command line:

```
sudo service synergy stop
```

2 Navigate to the following directory:

installDir/OpenManage/Network Manager/oware/synergy/conf

3 Copy the server-overrides.properties.sample file to server-overrides.properties.

4 Open the server-overides.properties file with a text editor.

5 Uncomment the show.portal.hints attribute.

6 Set the show.portal.hints attribute to false.

7 Restart the Web server.

For example, enter the following from the command line:

```
sudo service synergy start
```

8 Login and verify that the hint no longer shows.

Modifying Column Settings

You can make changes to the columns that are displayed, including to show additional columns, hide certain columns, change the column left-to-right orientation shown, or change the column width.

Modify column settings from an expanded or summary portlet as follows.

1 Click the Settings tool.

The Settings window is displayed.



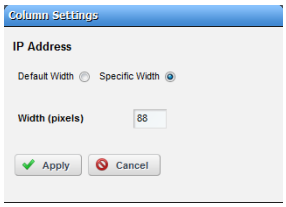
2 Click the Columns tab.

All data attributes that are available for the portlet are displayed.

3 Click the appropriate button to show/hide a column.

If you select to show a column, the settings option is activated, where you specify column width.

4 Click Settings to change the column width settings as needed.



5 Change the order in which columns appear using drag-and-drop.

The top-to-bottom attribute orientation corresponds to the left-to-right column orientation within the portlet.

6 Click Apply and exit the window.

The changes appear instantaneously when you return to the portlet.

Defining Advanced Filters

Among other places, filters appear at the top of expanded portlets. Many pre-installed filters come from driver packages you installed. Filters match vendors and/or entity types, but may not necessarily make sense in the context of a particular portlet. You can pick filters from already-configured filters list, or click Advanced and create your own filter.

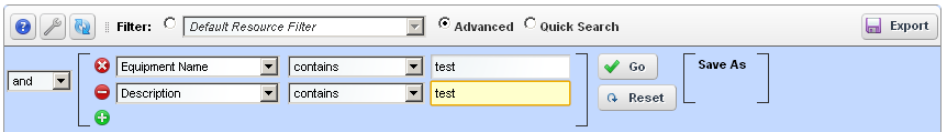
NOTE:

You can also filter what appears on a page with the Container View Portlet. Select a container, and the rest of the portlets on that page confine displayed data to reflect the selected container's contents.

Define advanced filters as follows.

1 Select Advanced.

The advanced filter fields and options are displayed.



2 Select an operator (and/or) if combining more than one filter.

3 Provide the field, condition, and text to filter.

4 Click the add button (+) to define another filter.

5 Click Go to see the list after the filter acts on it.

6 Click Reset if you want to return the list to its original state.

7 Click Save As to preserve a filter you have configured for future use.

8 Enter a name and description.

9 Click *Save*

The new filter is now available from the Filter list.

See Redcell > Filter Management on page 685 for directions to the screen that catalogs all such filters.

Exporting/Importing Page Configurations

Export/Import also appears as a tab in screens that manage pages (*Manage* > *Page* and *Manage* > *Control Panel* screens display these tabs). For example, click *Manage* > *Settings* in the Dock. Use the options on the Export/Import page to select exactly what elements to export. The automated file name includes your login identity, the date, and the `lar` extension. The file itself is a compressed collection of XML file configuration settings for the Pages/Portlets you have elected export. Its destination is the browser's default download location. Use the *More Options* link at the bottom of the Export screen to expose more export options. Use this same page to import such exported files, if it is enabled for your user.

Sharing a Resource

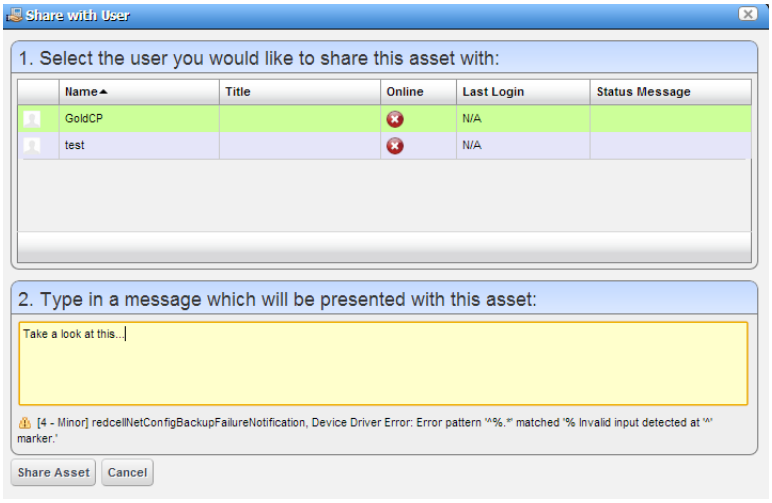
You can share elements within the OpenManage Network Manager (OMNM) system with colleagues when more than one user exists on your OMNM system, and consult with them using the conferencing described in Status Bar on page 444.

Share a resource with colleagues as follows.

1 Select a resource listed from the appropriate portlet.

2 Right-click and the select Share with User.

The Share with User window is displayed.



3 Select a user with whom you want to share.

4 Type any message you want to include.

5 Click Share Asset.

NOTE:

Sharing can only handle one item so it uses the first one in the selection.

The chat message to the selected user includes your text and a link that opens to display the Widgets panel for the selected item.

Editing Custom Attributes

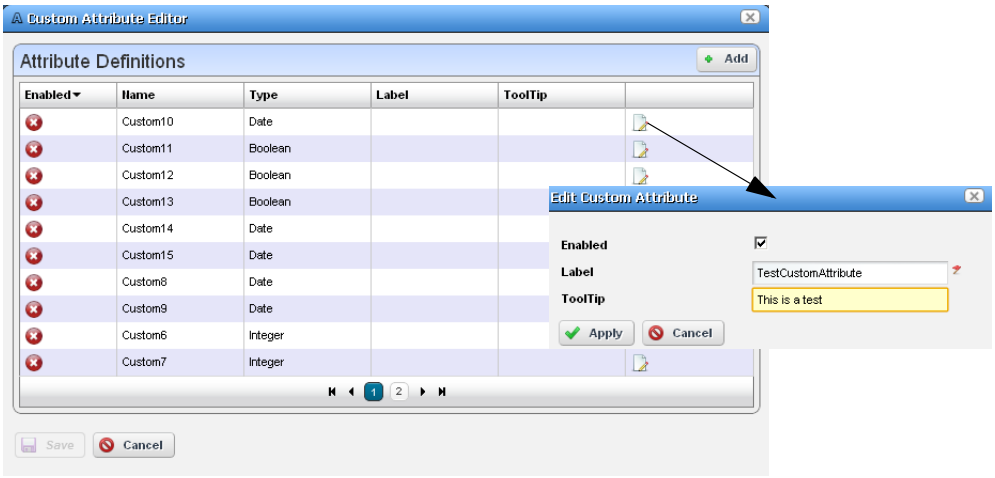
The Edit Custom Attributes pop-up menu option is available from many portlets (Managed Resources, Port, Contact, Vendor, or Location),

Edit custom attributes as follows.

1 Right-click the items whose attributes you want to modify.

For example, right-click an alarm from the Alarms portlet.

The Custom Attribute Editor displays the definitions appropriate for your selection. See Redcell > Data Configuration on page 682 for another way to get to this editor.



2 Click the edit tool.

3 Select Enable to activate the custom field.

4 Enter a label and optional tooltip.

The label is for the tooltip and is what you see in the portlets appropriate for the entity type you have selected. The tooltip that appears when you hover the cursor over the custom field.

NOTE:

Tooltips do not always function where the custom attribute appears in the Web client. However, even If it does not appear, other views, Web services, or reports may use it.

5 Click Apply.

6 Click Save to preserve any changes you have made.

7 Verify that the Custom Attributes panel now exists.

a. Right-click a resource.

b. Select Edit.

c. See if the Custom Attributes tab exists in the Extended Details.

d. a resource and look in the Extended Details/Custom Attributes panel to see them.

NOTE:

If you want to enter the longitude and latitude for your OpenManage Network Manager installation, go to Control Panel's Redcell > Application Settings to enter the information as a default location.

Configuring Job Viewer's Appearance

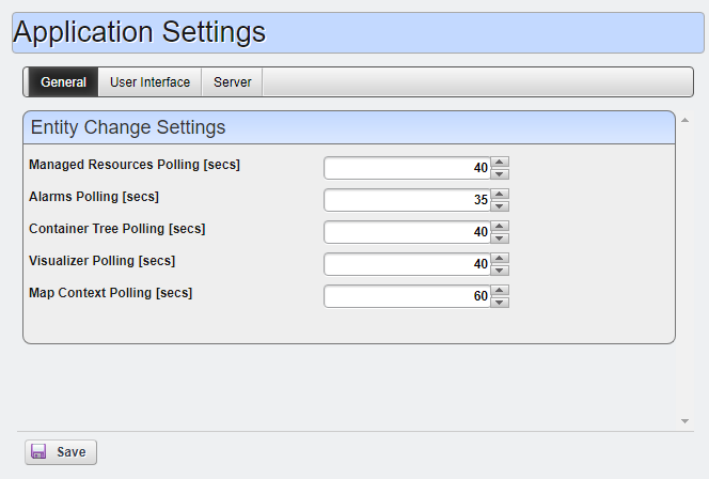
Configure the Job Viewer appearance as follows.

1 Select Go to > Control Panel.

The Control panel is displayed.

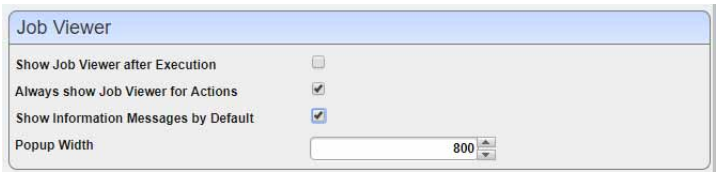
2 Select Redcell > Application Settings.

The General application settings are displayed.



3 Select the User Interface tab.

4 Go to the Job Viewer options.

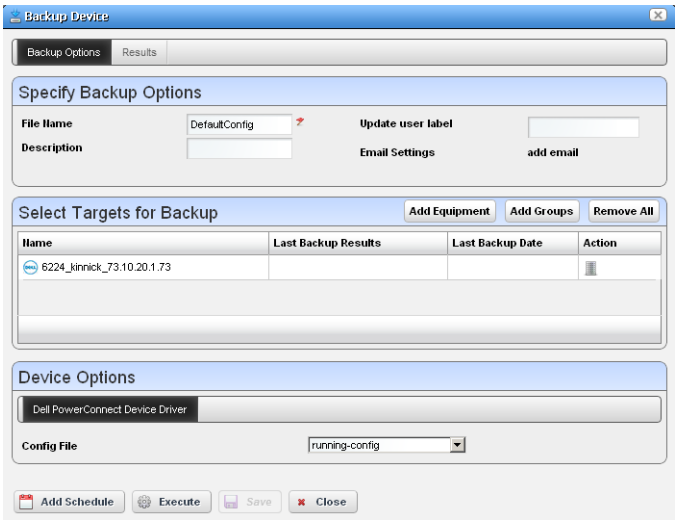


5 Select any of the following options that apply:
   - Show Job Viewer after Execution
   - Always show Job Viewer for Actions
   - Show Information Messages by Default
6 Change the pop-up width if needed.

Scheduling Actions

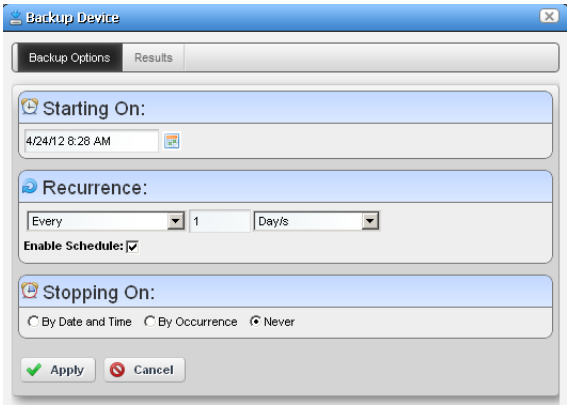
Schedule an action rather than execute it immediately, for example from Managed Resource portlet, follow these steps:

1 Select the action in the right-click menu. For example: device Backup.



2 Click Add Schedule instead of Execute.

The schedule panel appears.



Configure the start time and date, recurrence, and stop parameters in this screen. The *Results* tab displays an audit trail when the action executes.

3 Click *Apply*.

The previous panel returns, the *Add Schedule* button now appearing as *Edit Schedule*.

4 Click *Save*.

OpenManage Network Manager creates a scheduled item around the activity and its data. A row also appears in the screen described in Schedules Portlet on page 649 for this schedule.

When you have scheduled something from the *Add Schedule* button, clicking *Apply* in the schedule panel returns you to the previous screen.

If you click *Execute* in that previous screen, the action begins, and the audit trail panel appears, displaying the running job for the activity. If you have attached a Schedule, OpenManage Network Manager also saves the activity as a scheduled item in the Schedules Portlet.

3

Customizing Events and Alarms

This section provides tasks and information related to customizing events and alarms and understanding alarm propagation and event/alarm life cycles.

Setting Audible Alerts – 94
Creating Event Processing Rules – 95
Extracting Adaptive CLI Attributes from a Syslog Alarm – 104
Using Extended Event Definitions – 114
Understanding Alarm Propagation to Services and Customers – 119
Understanding Event Life Cycle – 122
Understanding Alarm Life Cycle – 125

Setting Audible Alerts

Audible Alerts produce a sound when a new alarm arrives in the Alarms summary (not expanded) portlet. The sound occurs when the OpenManage Network Manager (OMNM) auto-refresh controller polls for state changes. If you enable Audible Alerts and the Alarms summary view receives **new** alarms, the specified sound occurs.

Cleared alarms do not trigger an audible alert. **Only new** alarms received trigger an audible alert during auto-refresh. To cut down on audio clutter, only a single Audible Alert sounds no matter how many alarms occur during an auto-refresh cycle.

Each browser supports sound differently because of licensing for various sound formats. Audible alarm support exists for most browsers, so if issues occur with a particular browser the workaround is either to upgrade or use Chrome.

Browsers support MP3 sounds the most, so this is the only format supported for Audible Alerts. The Firefox browser only support OGG format natively and the Internet Explorer browser has issues with most sounds. To support those browsers, the OMNM application plays MP3 sounds through a Flash Object, so browsers need no special plugins.

This section provides instructions for:

- Turning On Audible Alerts
- Adding Custom MP3 Sounds

Turning On Audible Alerts

Turn on Audible Alerts as follows.

1 Navigate to the page containing the Alarms portlet.

NOTE:

For audible alerts to work, the Alarms portlet **must be** on a page without the Container View or other context broadcasting that dynamically changes the Alarms portlet's context. Auto refresh does not run when in this environment so as a result the Audible Alerts are not exposed. (See Understanding Containers on page 144.)

2 Click the Settings (wrench) tool.

The Setting window is displayed.

3 Enable the audible alerts for new alarms option.

This activates the sound field.

4 Select a sound to plays.

5 Click the play button to preview the selected sound.

By default, the OpenManage Network Manager product ships with four standard alert sounds: Alert, Bell, Chord, and Ding. See Adding Custom MP3 Sounds to add custom sounds.

6 Click Apply.

This Alarms portlet instance now has Audible Alerts enabled.

Adding Custom MP3 Sounds

Add custom MP3 sounds as follows.

1. Go to the Control Panel.
2. Click the Documents and Media section.
3. Click the Add button and then Select Basic Document.
4. Click Choose File and pick an MP3 file to upload from the File section.

   Because this interface lets you add any type of media, no file validation occurs. However, Audible Alerts only display audio/MP3 mime-types.
5. Give the new MP3 sound a short title.

   For example, if you upload cowsound.mp3, call it Cow Sound.
6. Click Publish.
7. Go back to the Alarms portlet.
8. Click the Settings (wrench) tool.
9. Verify that there is a new sound to select.

Creating Event Processing Rules

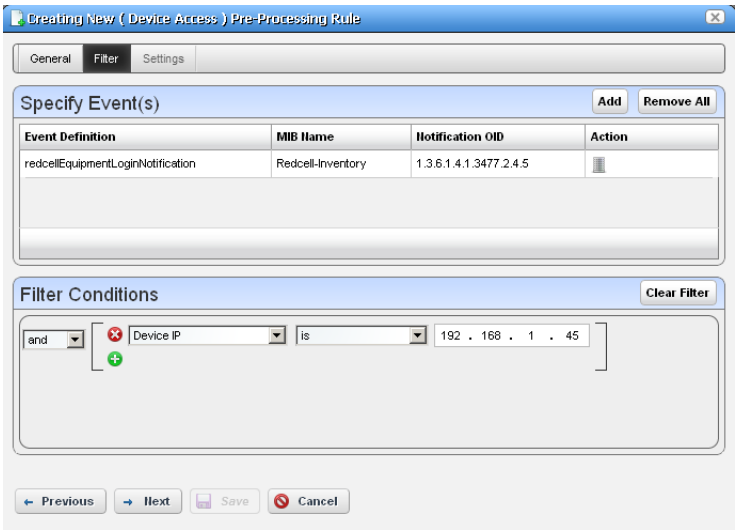
There are many different types of rules you can create. As an example, the steps provided show how to create a device access rule from the Automation and Event Processing Rules portlet. If you need a detailed description of this portlet, the rule types, or other menu option, see Automation and Event Processing Rules on page 512. Also see Filtering/Settings on page 486, Syslog Escalation Criteria on page 489, and Actions on page 493 for more about the differences available between rule types.

Create a rule from the Automation and Event Processing Rules portlet as follows.

1. Right-click and then select Event Definition Override > Device Access.

   The Rule Editor is displayed.
2. Enter a name to identify the rule and an optional description.
3. Select Enabled if you want this rule to begin working immediately.

4 Click Next to specify filters.



5 Add the events to filter.

a. Click Add to show the events list.

b. Select the events you want to add.

c. Click Add Filter to further filter the selected events.

See Expanded Portlet on page 450 for more about this feature.

6 Click Next to specify the settings for the selected rule type.

This panel's appearance depends on the type of rule you selected when you clicked New. When you are editing an existing rule, it defaults to that rule's screen. For more about the available alternatives, see Filtering/Settings on page 486.

The Device Access example creates a specific device access event for user login, logout, login failure, or configuration change.

7 Select the Access Type (Config Change, Login Failure, User Login, User Logout) from the pick list for that field.

8 Enter the User Name Variable and/or User Name RegEx match string.

This confines rule response to the selected users.

9 Select Suppress Correlated events if you do not want to see events correlated with this one.

10 Click Save to preserve the event processing rule.

NOTE:

To test these rules, you typically need specialized trap-sending software. However, you can make a rule respond to an internal OpenManage Network Manager event, such as backup failure if you only want to see the outcome. Simply disable your FTP server) and back up a device to get a backup failure event.

Forwarding Traps

SNMPv1 and SNMPv3 traps become SNMPv2 Traps

SNMPv1 traps are converted according to the RFC 1908 specification. SNMPv3 traps are already in the SNMPv2 format and the application simply does not use SNMPv3 security when sending these northbound. The following is the relevant snippet from the RFC 1908 specification:

```
3.1.2. SNMPv1 -> SNMPv2

When converting responses received from a SNMPv1 entity acting in an agent
    role into responses sent to a SNMPv2 entity acting in a manager role:

(1) ...

(2) If a Trap-PDU is received, then it is mapped into a SNMPv2-Trap-PDU.
    This is done by prepending onto the variable-bindings field two new
    bindings: sysUpTime.0 [6], which takes its value from the timestamp
    field of the Trap-PDU; and, snmpTrapOID.0 [6], which is calculated as
    follows: if the value of generic-trap field is enterpriseSpecific,
    then the value used is the concatenation of the enterprise field from
    the Trap-PDU with two additional sub- identifiers, '0', and the value
    of the specific-trap field; otherwise, the value of the corresponding
    trap defined in [6] is used. (For example, if the value of the generic-
    trap field is coldStart, then the application uses the coldStart trap
    [6]) Then, one new binding is appended onto the variable-bindings
    field: snmpTrapEnterprise.0 [6], which takes its value from the
    enterprise field of the Trap-PDU. The destinations for the SNMPv2-Trap-
    PDU are determined in an implementation-dependent fashion by the proxy
    agent.
```

Despite this description, many vendors defined a trap for SNMPv2 and then had to support sending it as SNMPv1 protocol. The assembly of v2 OID from v1 enterprise and specific is supposed to include an extra zero (0) as in: enterpriseOID.0.specific. However, if a v2 trap is defined that has no '0' in it, it cannot be sent as v1 and converted back following the specifications.

Sending as Proxy

The OpenManage Network Manager (OMNM) application can forward a trap as though it came from a device (sourceIP spoofing) or act as an agent proxy according to the SNMP-COMMUNITY-MIB. If not sending as a proxy, the OMNM application forwards traps from an application server cluster as an SNMPv2 notification as though it is coming directly from the originating agent (device). This is a common and the desired behavior. Some operating systems prevent packet spoofing as a security measure so this behavior is optional.

If sending as a proxy, the OMNM application forwards the trap from the IP address given in the field adjacent to the Send as Proxy option when you select it. If you select the Send as Proxy option but leave the adjacent IP address blank, the OMNM application forwards the trap from the receiving mediation server as sourceIP.

The relevant excerpt from SNMP-COMMUNITY-MIB is:

```
--
-- The snmpTrapAddress and snmpTrapCommunity objects are included
-- in notifications that are forwarded by a proxy, which were
-- originally received as SNMPv1 Trap messages.
--
```

```
snmpTrapAddress OBJECT-TYPE
        SYNTAX  IpAddress
        MAX-ACCESS accessible-for-notify
        STATUS current
        DESCRIPTION
                "The value of the agent-addr field of a Trap PDU which
                is forwarded by a proxy forwarder application using
                an SNMP version other than SNMPv1.  The value of this
                object SHOULD contain the value of the agent-addr field
                from the original Trap PDU as generated by an SNMPv1
                agent."
 -- 1.3.6.1.6.3.18.1.3 --  ::= { snmpCommunityMIBObjects 3 }

snmpTrapCommunity OBJECT-TYPE
        SYNTAX  OCTET STRING
        MAX-ACCESS accessible-for-notify
        STATUS current
        DESCRIPTION
                "The value of the community string field of an SNMPv1
                message containing a Trap PDU which is forwarded by a
                a proxy forwarder application using an SNMP version
                other than SNMPv1.  The value of this object SHOULD
                contain the value of the community string field from
                the original SNMPv1 message containing a Trap PDU as
                generated by an SNMPv1 agent."
 -- 1.3.6.1.6.3.18.1.4 --  ::= { snmpCommunityMIBObjects 4 }
```

The OMNM application always adds `snmpTrapAddress` to every trap forwarded as a proxy, (never adding `snmpTrapCommunity`). It does not keep track of the community string on the traps received.

Forwarding a Generic Message

The option to forward a generic message forwards a trap or other type of message is found in the following MIB file:

```
../owareapps/eventmgmt/mibs/AssureAlarms-MIB
```

The following is the definition, as found in this file:

```
redcellGenericTrap NOTIFICATION-TYPE
OBJECTS { alarmOID, referencedNotificationTypeOID,
   referencedNotificationName, redcellSeverity, redcellEquipmentName,
   redcellEquipmentManagerOID, redcellInventoryEntityName,
   redcellInventoryEntityType, alarmMessage,
   redcellNotificationReceivedTime, redcellEquipmentIPAddress }
   STATUS current
DESCRIPTION
"Generic trap used for forwarding information about another trap while
   using a standard trap format and notification type OID."
::= { defaultProcessing 6 }
```

There is an XML version of this definition in the following file:

```
.../owareapps/eventmgmt/server/conf/mibs.xml
```

Here is the XML content, as found in this file:

```
<item>
    <Description>Generic trap used for forwarding information about another
       trap while using a standard trap format and notification type OID.</
       Description>
    <IndexPosition>1</IndexPosition>
    <Name>redcellGenericTrap</Name>
    <OID>1.3.6.1.4.1.3477.1.7.11.6</OID>
    <Status>current</Status>
    <Type>NOTIFICATION-TYPE</Type>
    <Variables>
        <item>
            <Name>alarmOID</Name>
            <OID>1.3.6.1.4.1.3477.1.7.11.1</OID>
        </item>
        <item>
            <Name>referencedNotificationTypeOID</Name>
            <OID>1.3.6.1.4.1.3477.1.7.11.3</OID>
        </item>
        <item>
            <Name>referencedNotificationName</Name>
            <OID>1.3.6.1.4.1.3477.1.7.11.4</OID>
        </item>
        <item>
            <Name>redcellSeverity</Name>
            <OID>1.3.6.1.4.1.3477.1.6.1</OID>
        </item>
        <item>
            <Name>redcellEquipmentName</Name>
            <OID>1.3.6.1.4.1.3477.2.3.1</OID>
        </item>
        <item>
            <Name>redcellEquipmentManagerOID</Name>
            <OID>1.3.6.1.4.1.3477.2.3.14</OID>
        </item>
        <item>
            <Name>redcellInventoryEntityName</Name>
            <OID>1.3.6.1.4.1.3477.2.1.8</OID>
        </item>
        <item>
            <Name>redcellInventoryEntityType</Name>
            <OID>1.3.6.1.4.1.3477.2.1.5</OID>
        </item>
        <item>
            <Name>alarmMessage</Name>
            <OID>1.3.6.1.4.1.3477.1.7.11.2</OID>
        </item>
        <item>
            <Name>redcellNotificationReceivedTime</Name>
            <OID>1.3.6.1.4.1.3477.1.6.3</OID>
        </item>
```

```
        <item>
            <Name>redcellEquipmentIPAddress</Name>
            <OID>1.3.6.1.4.1.3477.2.3.8</OID>
        </item>
    </Variables>
    <ViewType>OBJECT</ViewType>
</item>
```

Using Email Action Variables

The following are the Email Action variables used to customize the action email content. These variables are classified as follows:

- Basic Variables
- Managed Equipment Variables
- Entity Type: Port
- Entity Type: Interface, Logical interface

To successfully retrieve custom attributes in an e-mail, you must first create them. See Editing Custom Attributes on page 88.

You can also configure more limited variables that are slightly more efficient in performance, if not as detailed as those described in the following section.

For example, you can retrieve the following attributes:

```
{RedCell.Config.EquipmentManager_Custom1}
{RedCell.Config.EquipmentManager_Custom2}
{RedCell.Config.EquipmentManager_LastBackup}
{RedCell.Config.EquipmentManager_LastConfigChange} and
{RedCell.Config.EquipmentManager_HealthStatus}
```

NOTE:

If the entity does not contain/return these values, then the message [No data for <attribute name>] appears in the email instead.

Best practice is to clarify such attributes by combining them with others that spell out their source.

Basic Variables

Here is a description of the basic variables:

Attribute	Description	Email Action Variable
Name	The event / alarm name	{Name}
Message	Description from the event	{Message}
Entity Name	The entity (interface, card...) name	{EntityName}
Equipment Manager Name	The name of the equipment, parent or chassis.	{EquipMgrName}
Device IP address	the IP of the device in alarm	{DeviceIP}
Entity Type	Type of entity (Router, and so on)	{EntityType}
Instance ID	An identifier for the event	{InstanceID}
Protocol Type	Of originating alarm (SNMP, syslog, etc.)	{ProtocolType}
Protocol Sub Type	Inform, Trap, [blank] (for internal events)	{ProtocolSubType}

Attribute	Description	Email Action Variable
Receive Time		{RecvTime}
Region	The mediation server partition name.	{Region}
Severity	0 - cleared, through 6 - critical, from Alarm Definition	{Severity}
Source IP address	The IP of the component sending the alarm	{SourceIP}

Managed Equipment Variables

Here is a description of the managed equipment variables. These variables may have a performance impact.

Attribute	Description	Email Action Variable
Custom 1	Note that although you can re-name any Custom attribute, you must use the variable's original name. For example here, that is {RedCell.Config.EquipmentManager_Custom1}	{RedCell.Config.EquipmentManager_Custom1}
Custom 2		{RedCell.Config.EquipmentManager_Custom2}
Custom 3		{RedCell.Config.EquipmentManager_Custom3}
Custom 4		{RedCell.Config.EquipmentManager_Custom4}
Custom 5		{RedCell.Config.EquipmentManager_Custom5}
Custom 6		{RedCell.Config.EquipmentManager_Custom6}
Custom 7		{RedCell.Config.EquipmentManager_Custom7}
Custom 8		{RedCell.Config.EquipmentManager_Custom8}
Custom 9		{RedCell.Config.EquipmentManager_Custom9}
Custom 10		{RedCell.Config.EquipmentManager_Custom10}
Custom 11		{RedCell.Config.EquipmentManager_Custom11}
Custom 12		{RedCell.Config.EquipmentManager_Custom12}
Custom 13		{RedCell.Config.EquipmentManager_Custom13}
Description	Description of the equipment	{RedCell.Config.EquipmentManager_DeviceDescription}
DNS Hostname	Hostname of equipment	{RedCell.Config.EquipmentManager_Hostname}

Attribute	Description	Email Action Variable
Equipment Type	Equipment Type	{RedCell.Config.EquipmentManager_CommonType}
Firmware Version	Version of the equipment's firmware	{RedCell.Config.EquipmentManager_FirmwareVersion}
Hardware Version	Version of the equipment's hardware	{RedCell.Config.EquipmentManager_HardwareVersion}
Last Backup	Last Backup	{RedCell.Config.EquipmentManager_LastBackup}
Last Configuration Change	Last Configuration Change	{RedCell.Config.EquipmentManager_LastConfigChange}
Last Modified	Timestamp of Last Modified	{RedCell.Config.EquipmentManager_LastModified}
Model	Model number of the equipment	{RedCell.Config.EquipmentManager_Model}
Name	Component name	{RedCell.Config.EquipmentManager_Name}
Network Status	Network Status	{RedCell.Config.EquipmentManager_HealthStatus}
Notes	Equipment Notes	{RedCell.Config.EquipmentManager_Notes}
OSVersion	OSVersion	{RedCell.Config.EquipmentManager_OSVersion}
Serial Number	Unique identifier for the equipment	{RedCell.Config.EquipmentManager_SerialNumber}
Software Version	Version of the equipment's software	{RedCell.Config.EquipmentManager_SoftwareVersion}
System Object Id	SNMP based system object identifier	{RedCell.Config.EquipmentManager_SysObjectID}

Entity Type: Port

Here is a description of the Port entity type variables.

Attribute	Description	Email Action Variable
Custom 1	Note that although you can re-name any Custom attribute, you must use the variable's original name. For example here, that is {RedCell.Config.EquipmentManager_Custom1}	{RedCell.Config.Port_Custom1}
Custom 2		{RedCell.Config.Port_Custom2}
Custom 3		{RedCell.Config.Port_Custom3}
Custom 4		{RedCell.Config.Port_Custom4}
Encapsulation	Encapsulation	{RedCell.Config.Port_Encapsulation}
Hardware Version	Version of the port's hardware	{RedCell.Config.Port_HardwareVersion}
If Index	SNMP If Index	{RedCell.Config.Port_IfIndex}

Attribute	Description	Email Action Variable
MAC Address	"Typically a MAC Address, with the octets separated by a space, colon or dash depending upon the device. Note that the separator is relative when used as part of a query."	{RedCell.Config.Port_UniqueAddress}
Model	Model number of the port	{RedCell.Config.Port_Model}
MTU	Maximum Transmission Unit	{RedCell.Config.Port_Mtu}
Name	Port name	{RedCell.Config.Port_Name}
Notes	Port Notes	{RedCell.Config.Port_Notes}
Port Description	Description of the port	{RedCell.Config.Port_DeviceDescription}
Port Number	Port Number	{RedCell.Config.Port_PortNumber}
Slot Number	Slot Number	{RedCell.Config.Port_SlotNumber}
Speed	Speed	{RedCell.Config.Port_Speed}
Subnet Mask	SubMask	{RedCell.Config.Port_SubMask}

Entity Type: Interface, Logical interface

Here is a description of the Interface, Logical interface entity types:

Attribute	Description	Redcell Email Action variable
Custom 1	Note that although you can re-name any Custom attribute, you must use the variable's original name. For example here, that is {RedCell.Config.EquipmentManager_Custom1}	{RedCell.Config.Interface_Custom1}
Custom 2		{RedCell.Config.Interface_Custom2}
Custom 3		{RedCell.Config.Interface_Custom3}
Custom 4		{RedCell.Config.Interface_Custom4}
Encapsulation	Encapsulation	{RedCell.Config.Interface_Encapsulation}
IfIndex	SNMP Interface Index	{RedCell.Config.Interface_IfIndex}
Interface Description	Description of the Interface	{RedCell.Config.Interface_DeviceDescription}
Interface Number	Interface Number	{RedCell.Config.Interface_InterfaceNumber}
Interface Type	Common Interface Type	{RedCell.Config.Interface_CommonType}
MTU	Maximum Transmission Unit	{RedCell.Config.Interface_Mtu}
Name	Interface name	{RedCell.Config.Interface_Name}
Notes	Interface Notes	{RedCell.Config.Interface_Notes}
Port Number	Port Number	{RedCell.Config.Interface_PortNumber}
Slot Number	Slot Number	{RedCell.Config.Interface_SlotNumber}
Subnet Mask	Subnet Mask of the Interface	{RedCell.Config.Interface_SubMask}

Extracting Adaptive CLI Attributes from a Syslog Alarm

This section demonstrates how to pass attribute text from a syslog alarm to an action by detailing the following workflow:

1 Receiving Syslog Events

2 Matching Text from a syslogNotification Event

3 Creating Extended Event Definition for syslogNotification

4 Creating ACLI Action and Pass Varbind Value for Execution

5 Verifying the Results

Receiving Syslog Events

To receive syslog events, you need to configure a device to send syslog traps to the OpenManage Network Manager (OMNM) application.

Receive syslog events by configuring your device to send syslog traps to the OMNM application as follows.

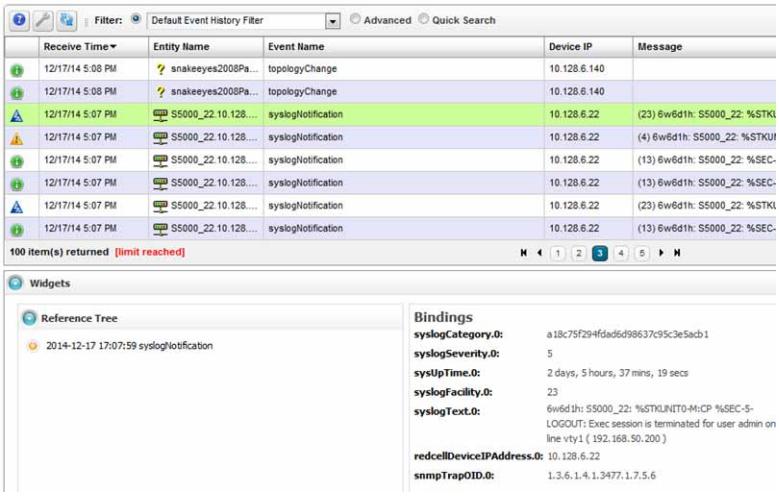
1 Configure a device to send syslog to the appserver.

For a Dell S5000 switch (10.128.6.22), add `logging 192.168.0.138`.

```
!
logging trap debugging
logging 192.168.54.43
logging 10.35.35.201
logging 10.35.35.78
logging 192.168.50.200
logging 192.168.0.138
```

2 Verify that the Event History portlet shows the SyslogNotification event name for the defined entity.

The syslogNotification default behavior is suppress. Because we receive many syslogNotifications, you can set the event to Reject after confirming the use case. For Cisco, the syslog event may use clogMessageGenerated.



Matching Text from a syslogNotification Event

This example matches specific text from an event and associates it to a category by creating a Syslog Escalation rule in the Event Processing Rule portlet.

Match text from a syslogNotification event as follows.

1 Extract the port information from a syslog message.

```
S5000> configure t
```

2 Log in Device and

```
> interface te 0/20
```

3 Shut down an interface:

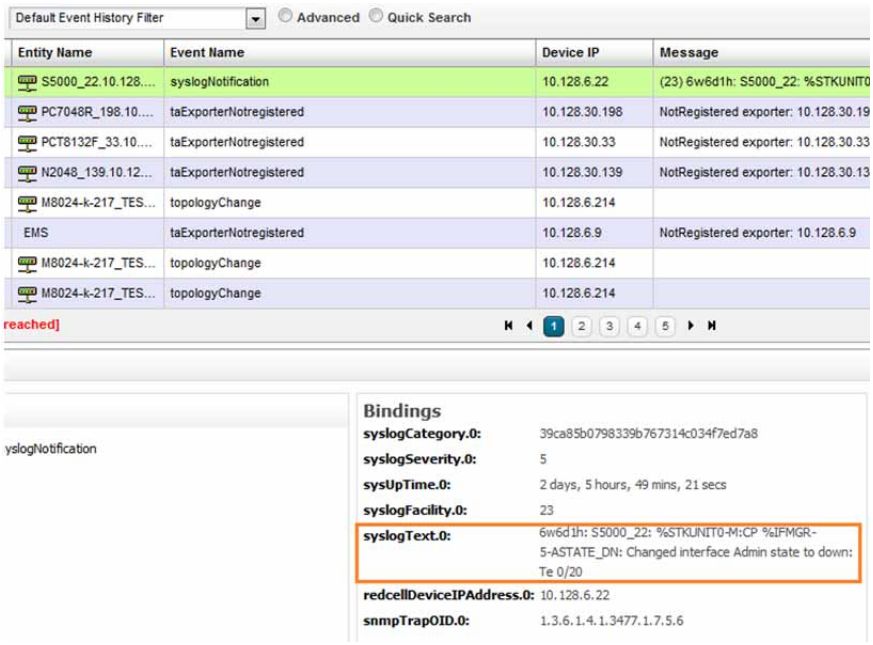
```
> shutdown
```

4 Bring up the interface

```
> no shutdown
```

5 Locate the `syslogNotification` event in the Event History portlet.

6 Look at the syslogText provided from the `shutdown` and `no shutdown` commands.



7 Extract the relevant port information with these messages.

```
syslogText.0: 6w6d1h: S5000_22: %STKUNIT0-M:CP %IFMGR-5-ASTATE_DN: Changed
    interface Admin state to down: Te 0/20
syslogText.0: 6w6d1h: S5000_22: %STKUNIT0-M:CP %IFMGR-5-ASTATE_UP: Changed
    interface Admin state to up: Te 0/20
```

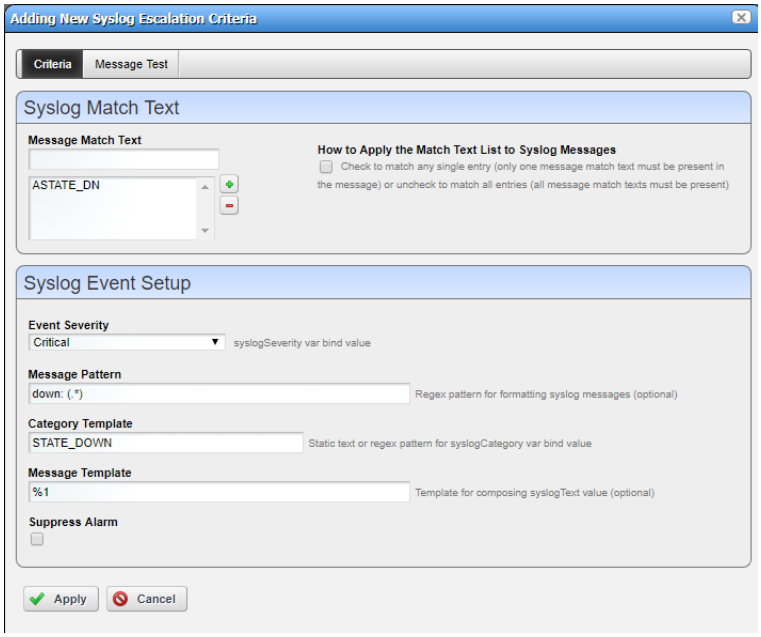
8 Right-click to create a new Protocol Translation > Syslog rule in the Event Processing Rules portlet to extract information.

9 Make sure that the filtering tab is not blank as you edit.

For this example set `Source IP is not 0.0.0.0.`

10 Add the Escalation criteria extracting the following Syslog information for the `Te 0/20` interface:

```
syslogText.0: 6w6d1h: S5000_22: %STKUNIT0-M:CP %IFMGR-5-ASTATE_DN: Changed
    interface Admin state to down: Te 0/20
```



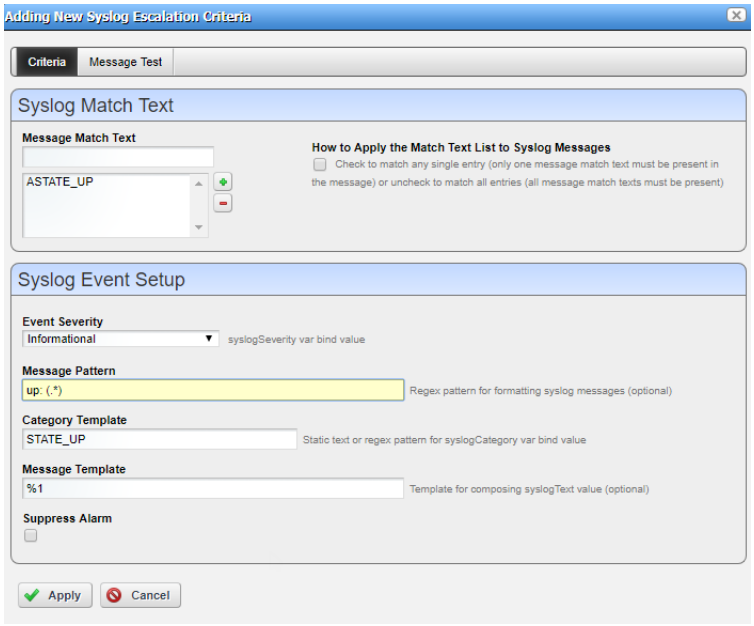
11 Provide the following information:

- **Message Match Text** use `ASTATE_DN` from the `syslogText`.
- **Event Severity** is the alarm severity for `syslogNotification::[Category]`
- **Message Pattern** get from the given `syslogText.0`, parse the port string (`Te 0/20`) with `down: (.*)`
- **Category** Template set up an event definition based on the Category name. The next step creates an Extended Event Definition for this. For example, the next time this type of syslog alarm arrives, it appears as `syslogNotification::[Category]` in this case `syslogNotification::STATE_DOWN`.
- **Message Template** is the regular expression in this rule parses *Message Pattern*, %1 from `(.*)` into `syslogText`

12 Apply the STATE_DN criteria.

13 Parse the `ASTATE_UP` match text similar to:

```
syslogText.0: 6w6d1h: S5000_22: %STKUNIT0-M:CP %IFMGR-5-ASTATE_UP: Changed
    interface Admin state to up: Te 0/20
```



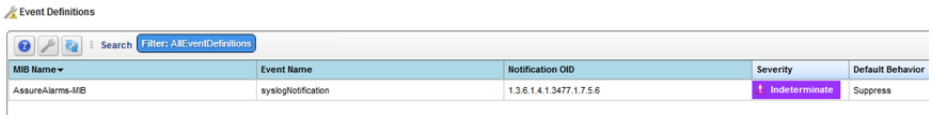
14 Apply and then Save.

Creating Extended Event Definition for syslogNotification

Create extended event definition events to associate certain alarms for syslogNotification categories.

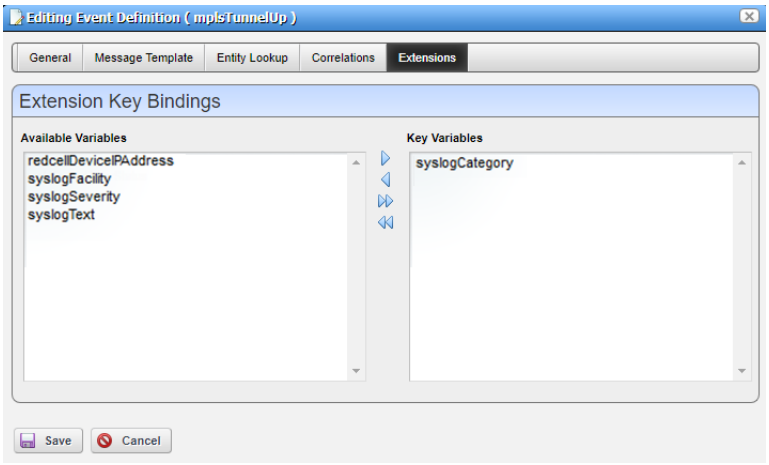
1 Go to the Event Definitions portlet (Settings > Alarm Definitions).

2 Locate the syslogNotification event.



3 Right-click the syslogNotification event and then select Edit.

The Editing Event Definition window is dispalyed.



4 Click the Extensions tab.

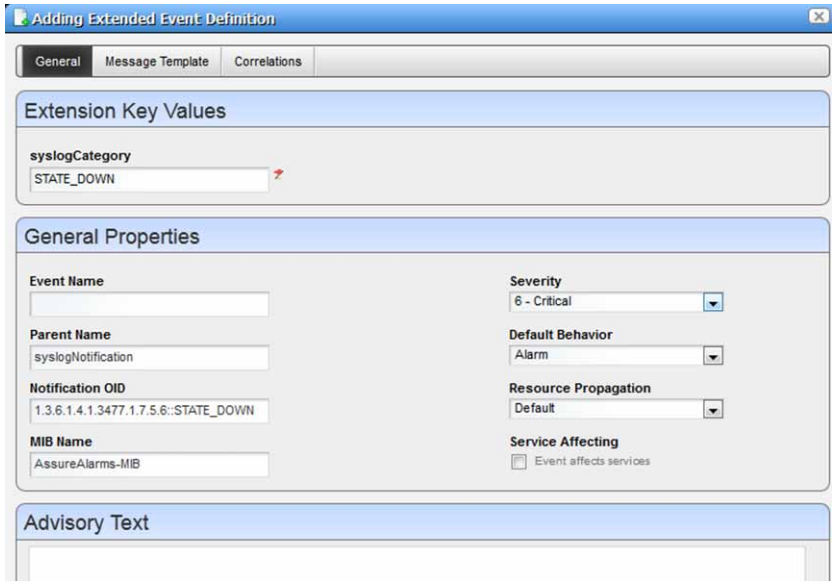
5 Add syslogCategory to the Key Variables list.

6 Click Save.

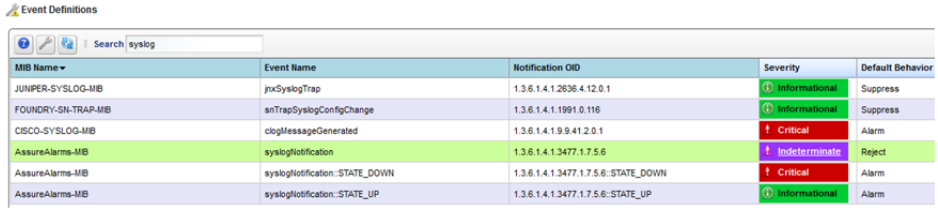
7 Right-click the syslogNotification event and then select Add Extended Event Definition0.

The Adding Extended Event Definition window is displayed.

8 Use the category specified earlier and have `syslogCategory` create the Extended Event Definition.



9 Verify that the next alarm is the alarm created during this exercise, after creating the syslog events for syslogNotification::STATE_DOWN and STATE_UP.

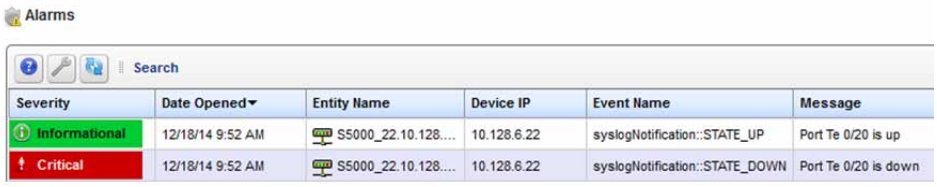


10 Log into the device and shutdown an interface and then check the Alarms or Event History:

```
S5000> configure t
> interface te 0/20
> shutdown
```

Then bring up the interface:

```
> no shutdown
```



Creating ACLI Action and Pass Varbind Value for Execution

For this example, create an ACLI action to bring up the interface based on the Varbind extracted from the syslogNotification event. So if you shut down an interface, what we did previously extracted the port information into the syslogText attribute, the Adaptive CLI uses the Varbind for the ACLI script we set up here.

Create an ACLI action pass the Varbind value for execution as follows.

1 Navigate to the Actions portlet (Resources > Actions).

1 Create a new action.

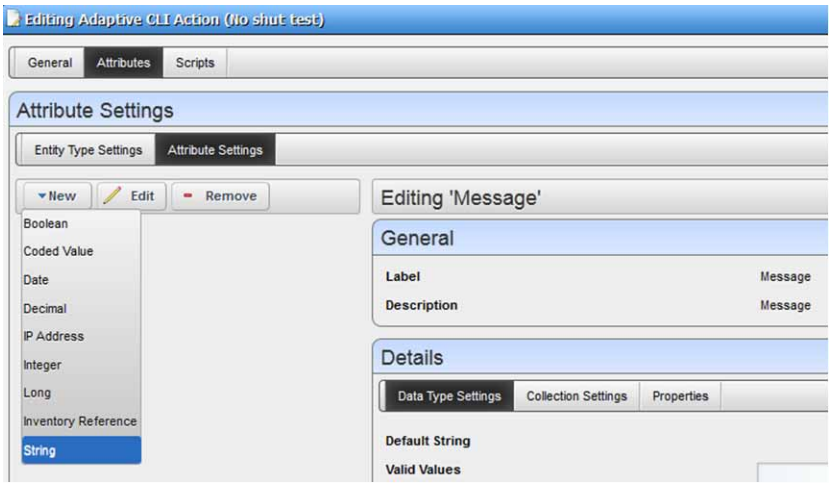
   a. Right-click the portlet and then select New > Adaptive CLI.

   b. Specify the general settings and any associated actions.

   c. Save the action.

2 Select the Attributes tab.

3 Create a String attribute `Message`.



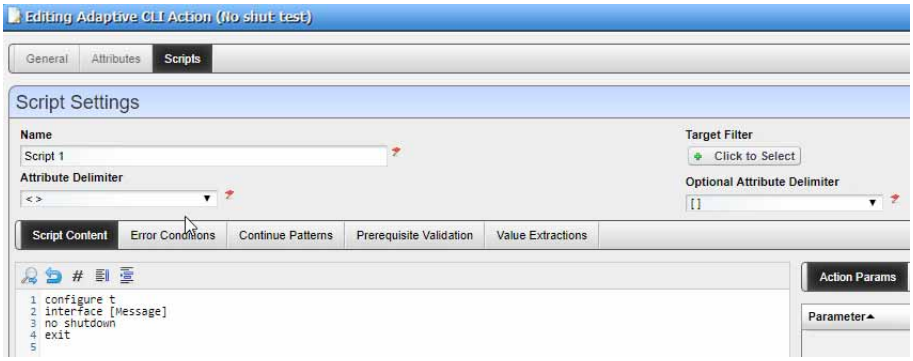
4 Select the Scripts tab.

5 Create an Embedded CLI script.

   For example, enter the following commands:

```
configure t
interface [Message]
no shutdown
exit
```

We will create a post processing rule and pass a Varbind OID so it goes into the Message parameter specified here.



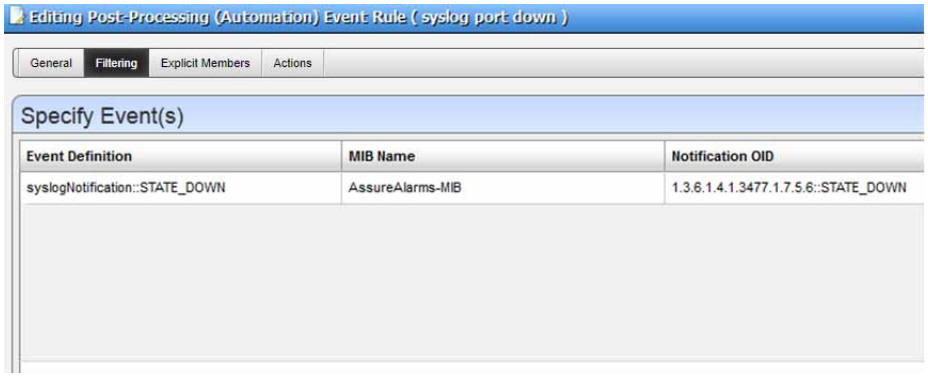
6 Create an Automation rule.

a. Select Alarms > Automation.

The Automation and Event Processing Rules portlet is displayed.

b. Right-click and then select New > Automation.

c. Add the event with which to trigger an action.



d. Click the Actions tab and then select Add Action > Action.

e. Select the action you made.

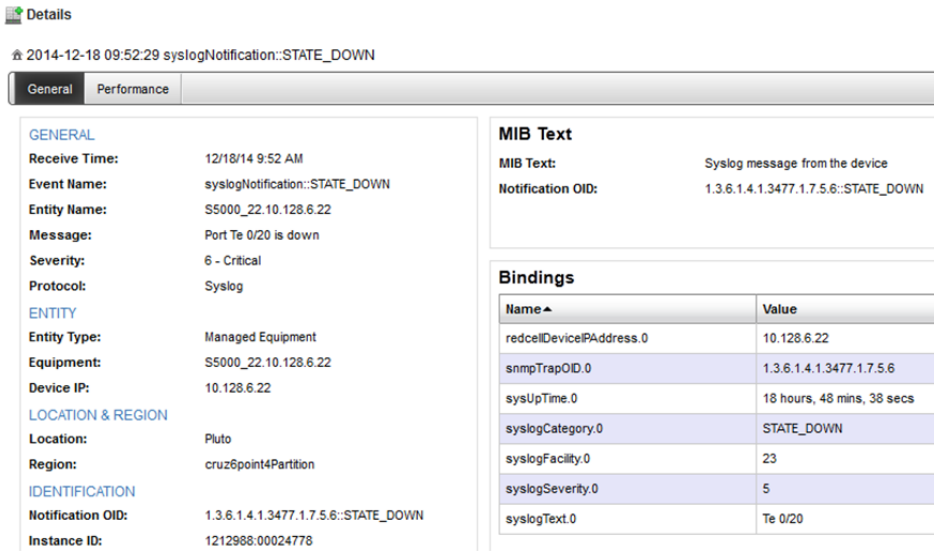
f. Pass the Varbind OID to the Adaptive CLI action.

For a Varbind, the syntax is `[[VARBIND: <varbind_oid>]]`.



The Varbind of interest is the syslogText extracted port string from syslogNotification.

7 Check the Event Details from Event History portlet.



8 Get the Varbind OID.

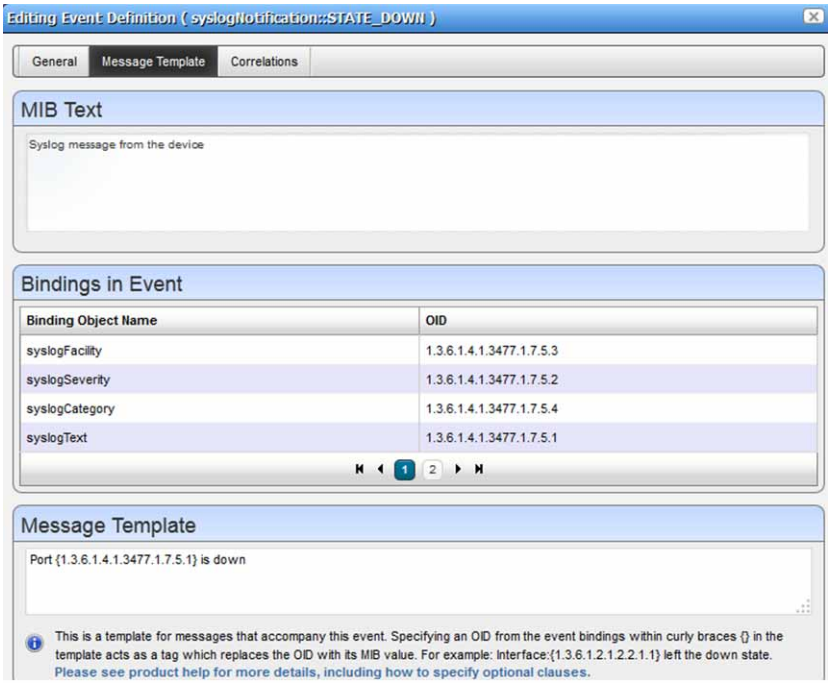
a. Go to the Event Definition portlet (Settings > Alarm Definitions).

b. Right-click the event definition and then select Edit.

The Editing Event Definition window is dispalyed.

c. Click the Message Template tab.

The syslogText OID shows as `1.3.6.1.4.1.3477.1.7.5.1`



Verifying the Results

Verify the results as follows.

1. Trigger the *syslogNotification::STATE_DOWN* event by shutting down an interface.

   If the Adaptive CLI action successfully brings the interface back up, it triggers the *syslogNotification::STATE_UP event*.

2. Check the audit trail for the Adaptive CLI action.

   When successful, it indicates the Adaptive CLI successfully used the syslogText varbind message.

Using Extended Event Definitions

To handle complex networks, you can configure event responses with a “Base Event Definition” and several “Extended Event Definitions” (EEDs). You can customize events, the reaction to them, and even extend events with EEDs. Modified or extended event definitions override the base set of definitions that comes from the traps and notifications found in loaded MIB files, and their OIDs appear in the Event Definition Editor on page 498.

You can modify Extended Event Definitions two ways:

- Extending Event Definitions
- Extending Event Definition XML

You can configure extended event definitions to perform partial matching on variable bindings by including **wildcard characters** in the extension key. The asterisk * matches any number of characters and the question mark ? matches a single character. For example an extension key of 1* matchs variable bindings that start with a 1 including 11, 12, 134, and so on. An extension key of 1? matchs 11, 12, 13 but does not match 134. An extension key of *3* matchs any variable binding that includes the number 3 somewhere, including 34, 13, 3, 438.

Extending Event Definitions

To extend event definitions, you create “child” events that extend a “parent” event. Extend an event definition as follows.

1. Save the parent event for which you configured Extensions.
2. Select it from the Event Definitions manager.
3. Right-click your selection and then select Add Extended Event Definition.

   The Adding Extended Event Definitions on page 505 window the Extension Key Values fields configured from the Event Definitions, Extensions panel. The variables also show in the order you selected from the Extensions panel. A suggested name for this event is the parent event name, followed by a colon-separated list of the field values entered on this screen.

Once configured, this extended event overrides the parent.

Extending Event Definition XML

After loading its base event definitions, the OpenManage Network Manager (OMNM) application loads all event definitions in the XML files in the server\conf directory under each module (for example \owareapps\redcell\server\conf\eventdefs.xml) and applies them as overrides. The OMNM application discards any XML event definitions if the notification type is unknown—that is, not in a loaded MIB. If you alter this XML file, you need to import it in Event Definitions Manager before the alterations take effect.

Extended event definitions (EEDs) support system extensions along with system overrides. An extension creates a unique definition for a MIB-based event that only applies to certain instances of the event. The extension appears as a separate event in the event definition manager and you can modify it as you can any other event.

Extension exist primarily to create specialized event definitions for recognizable variations from the basic event.

For details, see the following:

- XML Event Definition
- Extended Event Definitions
- Extended Event Definition Example

XML Event Definition

The format format is of an XML event definition:

```
<bean xsi:type="tns:NotificationDefinitionNP">
    <NotificationOID/>   <!-- required -->
    <ExtensionKey/>      <!-- extensions only - syntax: key1Value[:key2Value]-
        ->
    <Description/>       <!-- message text - supports object OID tag
        replacement: {objectOID} -->
    <Behavior/>          <!-- 1=alarm, 2=suppress, 3=reject (default is alarm)-
        ->
    <Severity/>         <!-- 0=clearing, 1=info, 2=unkown, 3=warning, 4=minor,
        5=major, 6=critical -->
    <ImpactPropagation/> <!-- 1=up, 2=down, 3=both (default is none) -->
    <KeyBindings>        <!-- OID(s) for bind object value(s) to use as
        correlation key -->
    <item/>
    </KeyBindings>
    <CorrelatedEvents>   <!-- OID(s) for alarms to clear when this event
        occurs. These OIDs can include an extension key as OID::extKey -->
        <item>oid[::keyValue[:keyvalue]]</item>
    </CorrelatedEvents>
</bean>
```

Extended Event Definitions

You can extend any event definition that defines one or more key bindings. The extension key consists of a value for each key binding in the correct order. You must separate each value with a colon (:).

Only extensions should set an extension key. The key format is dictated by the parent (extended) definition's key bindings. Set key bindings for the extension as needed for proper alarm correlation. The following Extended Event Definition Example provide some clarification.

NOTE:

Definition extensions do not inherit any settings from the extended definition.

Extended Event Definition Example

Events extend a basic definition:

```
bigBand 1.3.6.1.4.1.6387
```

Here are the extensions:

```
bigBandAdmin 1.3.6.1.4.1.6387::400
bigbandConfig 1.3.6.1.4.1.6387::5* (with partial matching extension key)
bigbandTraps 1.3.6.1.4.1.6387::400:50
bigbandAlarmTrapPrefix 1.3.6.1.4.1.6387::400:50:0
bigbandSessionAlarm 1.3.6.1.4.1.6387.400.50.0.0.2 (v2 OID)
bigbandEscalation 1.3.6.1.4.1.6387::400:50:0:0:3* (with partial matching
    extension key)
```

Another base event:

```
bigBandCommon 1.3.6.1.4.1.6387.100
```

Other extensions:

```
session 1.3.6.1.4.1.6387.100::50
sessionAlarms 1.3.6.1.4.1.6387.100::50:100
sessionAlarmTable 1.3.6.1.4.1.6387.100::50:100:40
sessionAlarmEntry 1.3.6.1.4.1.6387.100::50:100:40:1
sessionAlarmProgramNumber 1.3.6.1.4.1.6387.100::50:100:40:1:2
sessionAlarmEscalation 1.3.6.1.4.1.6387.100::50:100:40:1*:2? (with partial
    matching extension key)
```

The following example variables are for such extended events:

```
bigbandSessionAlarm TRAP-TYPE
    ENTERPRISE  bigbandAlarmTrapPrefix
    VARIABLES  {
        sessionAlarmAssertedTime,
        bigbandAlarmOnOrOff,
        sessionAlarmOutputChannelIndex,
        sessionAlarmProgramNumber,
        sessionAlarmPid,
        sessionAlarmAssertedType,
        sessionAlarmAssertedInputChannelIndexOrZero,
        bigbandSessionAlarmSequenceNo,
        sessionAlarmSessionId,
       sessionAlarmAuxiliary1,
       sessionAlarmAuxiliary2
    }
    DESCRIPTION
        "a session alarm is generated for every asserted/removed
         alarm. It contains all parameters as in sessionAlarm table,
         as well as a sequence no. that is incremented by 1 for
         every session-trap generation."
    ::= 2
```

The sample XML for the definitions and extensions:

```
<!-- bigbandSessionAlarm -->
  <bean xsi:type="tns:NotificationDefinitionNP">
    <NotificationOID>1.3.6.1.4.1.6387.400.50.0.0.2</NotificationOID>
    <Description>Program #{1.3.6.1.4.1.6387.100.50.100.40.1.2}</
   Description>
    <Behavior>1</Behavior>
    <Severity>2</Severity>
    <KeyBindings>
      <!-- bigbandAlarmOnOrOff -->
      <item>1.3.6.1.4.1.6387.400.50.1</item>
      <!-- sessionAlarmProgramNumber -->
      <item>1.3.6.1.4.1.6387.100.50.100.40.1.2</item>
    </KeyBindings>
  </bean>

  <!-- bigbandSessionAlarm ext:alarmOn program 12 -->
  <bean xsi:type="tns:NotificationDefinitionNP">
    <NotificationOID>1.3.6.1.4.1.6387.400.50.0.0.2</NotificationOID>
    <ExtensionKey>1:12</ExtensionKey>
    <Description>program #12 alarm ON</Description>
    <Behavior>1</Behavior>
    <Severity>4</Severity>
    <CorrelatedEvents>1.3.6.1.4.1.6387.400.50.0.0.2::0:12</
   CorrelatedEvents>
  </bean>

  <!-- bigbandSessionAlarm ext:alarmOff program 12 -->
  <bean xsi:type="tns:NotificationDefinitionNP">
    <NotificationOID>1.3.6.1.4.1.6387.400.50.0.0.2</NotificationOID>
    <ExtensionKey>0:12</ExtensionKey>
    <Description>Program #12 alarm OFF</Description>
    <Behavior>1</Behavior>
    <Severity>0</Severity>
    <CorrelatedEvents>1.3.6.1.4.1.6387.400.50.0.0.2::1:12</
   CorrelatedEvents>
  </bean>
```

To build on the previous BigBand example, the following example shows support for an EED with a partial key. It also shows the base event as an indeterminate severity alarm, then extends it for *alarm on* and *alarm off* default behaviors using partial keys. Finally, it is extended twice more, showing example of program-specific event settings.

```
<!-- bigbandSessionAlarm -->
  <bean xsi:type="tns:NotificationDefinitionNP">
    <NotificationOID>1.3.6.1.4.1.6387.400.50.0.0.2</NotificationOID>
    <Description>Program #{1.3.6.1.4.1.6387.100.50.100.40.1.2}</
   Description>
    <Behavior>1</Behavior>
    <Severity>2</Severity>
```

```
  <KeyBindings>
    <!-- bigbandAlarmOnOrOff -->
    <item>1.3.6.1.4.1.6387.400.50.1</item>
    <!-- sessionAlarmProgramNumber -->
    <item>1.3.6.1.4.1.6387.100.50.100.40.1.2</item>
  </KeyBindings>
</bean>

<!-- bigbandSessionAlarm ext: alarmOff all programs -->
<bean xsi:type="tns:NotificationDefinitionNP">
  <NotificationOID>1.3.6.1.4.1.6387.400.50.0.0.2</NotificationOID>
  <ExtensionKey>0</ExtensionKey>
  <Description>Program #{1.3.6.1.4.1.6387.100.50.100.40.1.2}</
 Description>
  <Behavior>1</Behavior>
  <Severity>0</Severity>
</bean>

<!-- bigbandSessionAlarm ext: alarmOn default -->
<bean xsi:type="tns:NotificationDefinitionNP">
  <NotificationOID>1.3.6.1.4.1.6387.400.50.0.0.2</NotificationOID>
  <ExtensionKey>1</ExtensionKey>
  <Description>Program #{1.3.6.1.4.1.6387.100.50.100.40.1.2}</
 Description>
  <Behavior>1</Behavior>
  <Severity>6</Severity>
</bean>

<!-- bigbandSessionAlarm ext: alarmOn program 12 -->
<bean xsi:type="tns:NotificationDefinitionNP">
  <NotificationOID>1.3.6.1.4.1.6387.400.50.0.0.2</NotificationOID>
  <ExtensionKey>1:12</ExtensionKey>
  <Description>program #12 alarm ON</Description>
  <Behavior>1</Behavior>
  <Severity>4</Severity>
</bean>

<!-- bigbandSessionAlarm ext: alarmOn program 40 -->
<bean xsi:type="tns:NotificationDefinitionNP">
  <NotificationOID>1.3.6.1.4.1.6387.400.50.0.0.2</NotificationOID>
  <ExtensionKey>1:40</ExtensionKey>
  <Description>#40 special message text</Description>
  <Behavior>1</Behavior>
  <Severity>5</Severity>
</bean>
```

Understanding Alarm Propagation to Services and Customers

The following describes the use cases where Alarm Propagation services and customers occurs. This describes the sequence of events/alarms. See also Variable Binding Definition Editor on page 636 for ways to augment propagation possibilities.

Alarm state must propagate to associated entities for each step and might take some time to reach all of them, so matching mentioned may not be instantaneous, depending on the complexity of the associations. This propagation to services and customers occurs through a background process, running on regular intervals.

A resource can have several levels of services that depend on it, and then customers can depend on them, and so on. Potentially, several levels of dependency and a large database full of services and customers to propagate alarm states can exist, so propagation processing occurs in the background. By default, this process runs every 30 seconds, but you can configure this interval by setting the com.dorado.assure.propagation.AlarmPropagationInterval property. This value is in milliseconds. For example, the to set the interval to 60 seconds, set this property as follows:

```
com.dorado.assure.propagation.AlarmPropagationInterval=60000
```

To prevent any OpenManage Network Manager upgrades from overwriting this setting, it is best to put it into the following file:

```
\owareapps\installprops\lib\installed.properties
```

After changing this property, make sure that you restart the application server for the change to take effect.

NOTE:

Only services associated with the alarmed subcomponents are affected by alarms on the subcomponent, not services connected to the rest of the device. You can also override default service affecting alarm behavior with an Event Processing Rule. See Automation and Event Processing Rules on page 512 for more details about this editor.

The remainder of this section describes what happens when a new alarm arrives, an existing alarm clears, or user actions execute.

A New Alarm Arrives

When a new alarm arrives, here is what happens:

What Happens	Description
Service Affecting Alarm Changes Source Alarm State:	The new alarm changes the alarm state (higher or lower) of the resource that is its source. **Dependencies:** If this resource has services or customers that depend on it, the alarm state matches for all such deployed, dependent services and their associated customers. Without such dependencies, no alarm state changes, besides that of the source.
Parent Resources:	The alarm changes the alarm state of a child of the source and the alarm's Resource Propagation value is Impacts Subcomponents. **Dependencies:** Child equipment matches the top level's alarm state. All deployed services and their related customers depending on this particular resource component match the resource component's alarm state.

What Happens	Description
Child Resources:	The alarm changes the alarm state of parent of the source and the alarm's Resource Propagation value is Impacts Top Level. **Dependencies:** Parent equipment matches the child entities alarm state. All deployed services and associated customers depending on only this resource's alarmed component have their alarm state match the resource's component.
No Change to Alarm State:	The new alarm does not change the alarm state of its source, so no services or customers have their alarm state changed
Alarm not Service Affecting:	The new alarm is not service affecting. The result is that no change occurs to services' or customers' alarm state.

Existing Alarm Clears

When an existing alarm clears, here is what happens:

What Happens	Description
Clearing Service Affecting Existing Alarm Changes Alarm State:	This changes the alarm state (higher or lower) of a resource. **Dependancies:** All deployed services and associated customers depending on this resource have their alarm state match the resource.
No Dependencies:	No services or customers change their alarm state
Clearing Non-Service Affecting Existing Alarm:	No services or customers have their alarm state changed

User Actions Execute

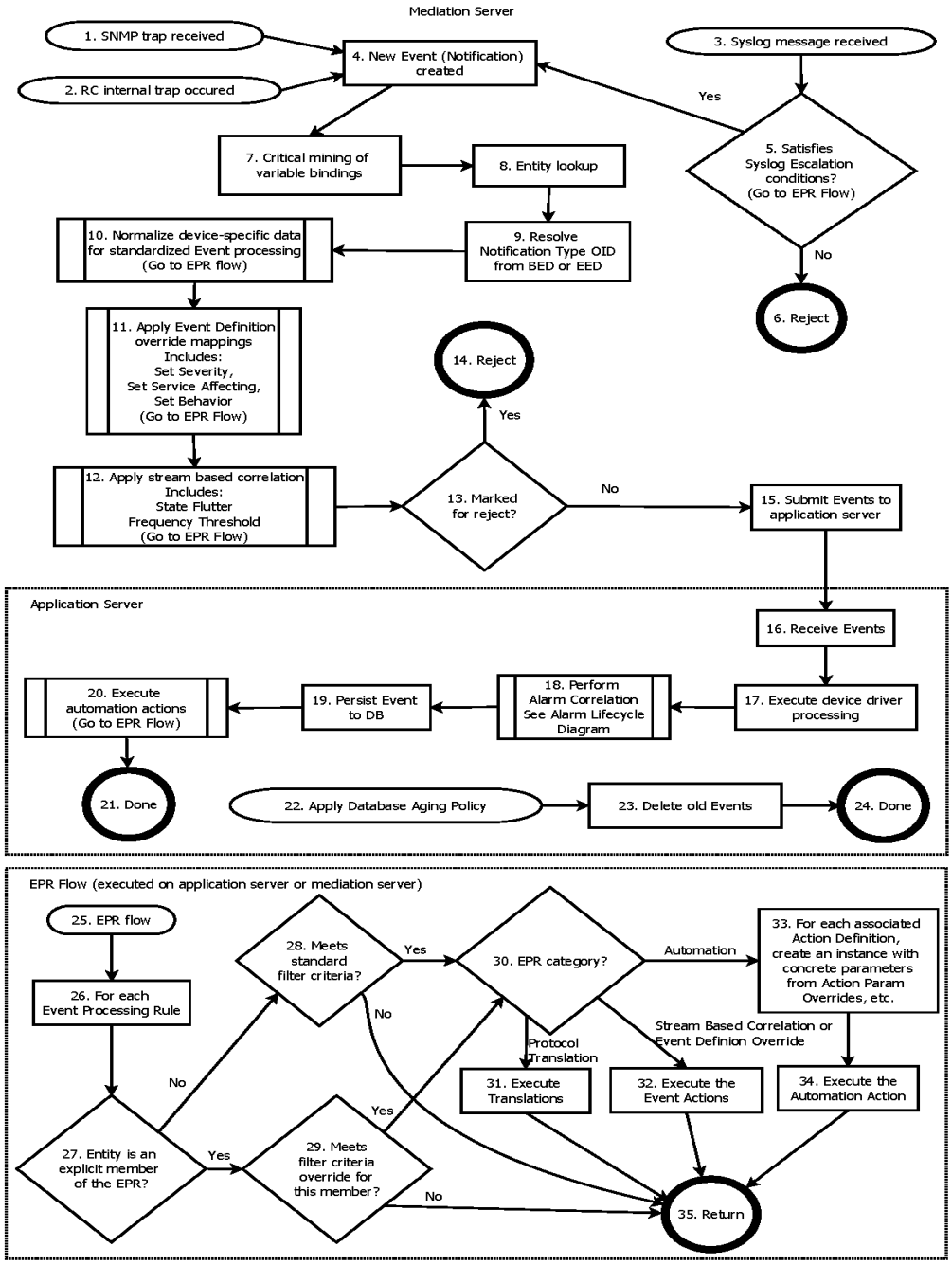
When user actions execute, here is what happens:

What Happens	Description
Resync the resource's alarm state:	• If the resource's displayed alarm state was incorrect, perhaps because it is a parent or child of a resource whose alarm state has changed, then this corrects it. • If this action changes the alarm state and this resource's most severe alarm is service affecting, then resync makes alarm states propagate to any associated services and customers. If the deployed services have the incorrect alarm state, then resync corrects that inaccuracy.
Viewing alarms associated with a service:	• If the service is deployed, and the target resource has open service affecting alarms, all open service affecting alarms for the target resource appear. • If the service is deployed, but the target resource has only cleared or non-service affecting alarms against it, no alarms appear. • If the service is deployed, and the target resource does not have open service affecting alarms, but at least one descendent entity of this resource has open service affecting alarms against it, those alarms propagate up to the resource. All open service affecting alarms that propagate up (Resource Propagation is *Impacts top level*) for the target resource's descendants appear • If the target resource does not have service affecting alarms, and neither do any service affecting alarms exist for its descendent entities, no alarms appear. • If the service is undeployed, no alarms appear.

What Happens	Description
Viewing alarms associated with a given customer:	• If at least one service associated with the customer has open, service affecting alarms, all open service affecting alarms for all services associated with this customer appear. • If none of the services associated with this customer have open, service affecting alarms, so alarms appear
User views the services impacted by a particular alarm:	• If the alarmed resource has at least one deployed service that depends on it, all deployed services depending on the alarmed resource appear. • If the alarmed resource does not have any deployed services that depend on it, no services appear.
Deploying a service whose target resource has service affecting alarms:	• Before deploying, no alarms appear for the service. After deploying, all open, service affecting alarms for the target resource appear.
Undeploying a service whose target resource has service affecting alarms:	• Before undeploying, all open, service affecting alarms for the target resource should appear. After undeploying, no alarms appear.
Editing a deployed service to change the target from one resource to another:	• If the original resource has service affecting alarms but the new one does not, all open service affecting alarms for the original target resource should appear before the edit. After the edit, no alarms appear. • If the original resource does not have service affecting alarms but the new one does, before editing, no alarms appear. After editing, all open service affecting alarms for the new target resource appear.

Understanding Event Life Cycle

The following diagram shows the OpenManage Network Manager events processing.



The following items correspond to the numbered processes in the diagram.

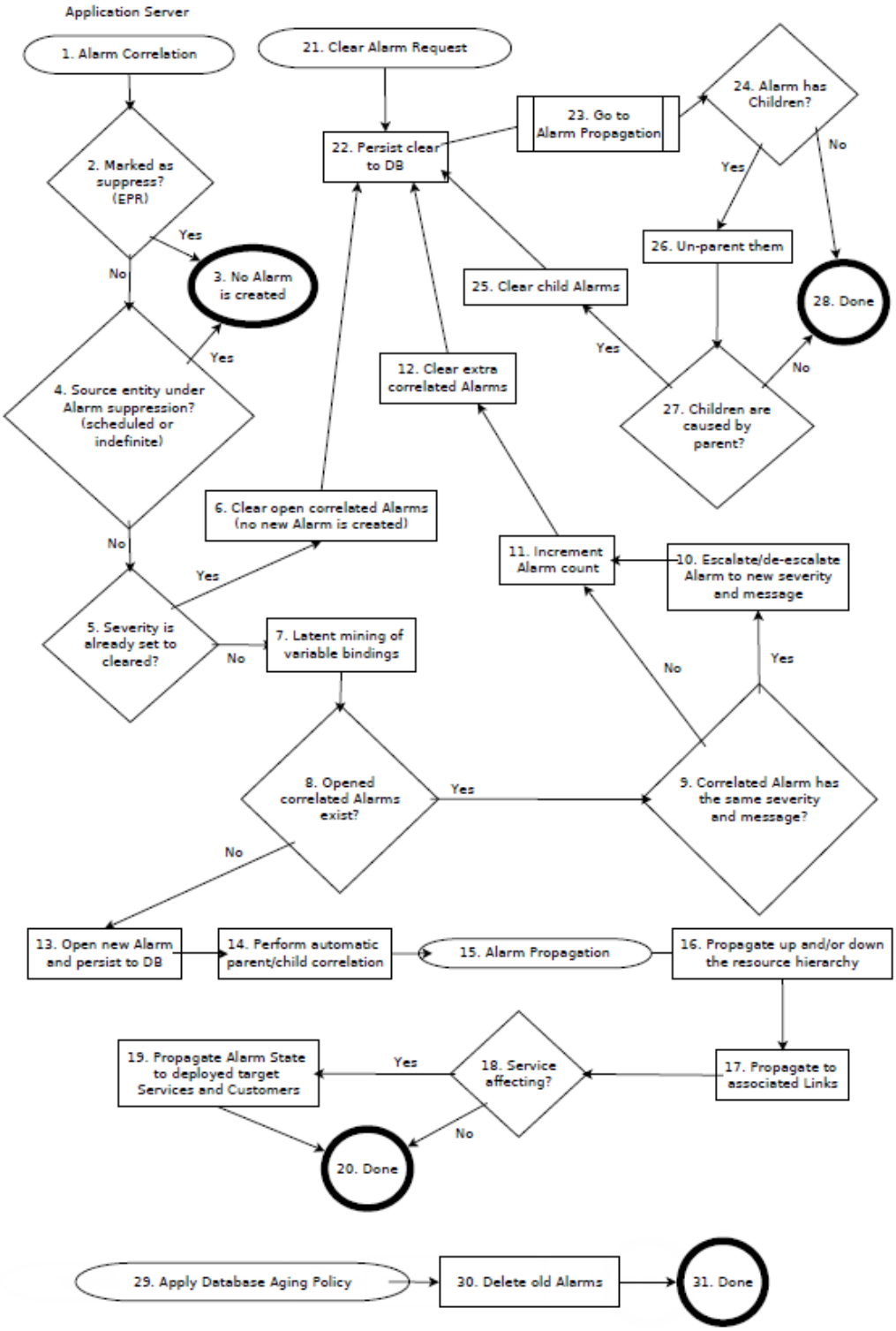
Process	Description
1 SNMP trap received	The server received an SNMP trap.

Process		Description
2	OpenManage Network Manager internal trap	An internal trap occurred within OpenManage Network Manager. Many situations are considered internal traps that emit an Event. One example is when a monitor polls a certain target and retrieves data for an attribute making the attribute cross a severity threshold. This emits a monitorAttributeTrend Event.
3	Syslog message received	The server received a Syslog message.
4	New Event (Notification) created	OpenManage Network Manager creates a new Event ("Notification") from the data received. Such Events are specific to OpenManage Network Manager's internal processing.
5	Satisfies filter conditions?	Syslog Event Processing Rules (EPRs) handle received Syslog messages to determine whether to convert the message into a OpenManage Network Manager Event or discarded. Such EPRs also determine how the Syslog data creates the new Event (what severity, message, and so on, it has).
6	Reject	If the received Syslog message does not satisfy the filter conditions of the Syslog EPRs then it is rejected and no Event occurs.
7	Critical mining of variable bindings	Sometimes OpenManage Network Manager must return to the device that sent the original trap to "mine" additional variable bindings. This mining can be either critical or latent, depending on whether OpenManage Network Manager needs the additional information early in the Event life cycle or whether it can wait until after an Alarm has been created. If OpenManage Network Manager needs additional data to associate an Event to an entity (which happens in #8. Entity lookup) then this is critical. On the other hand if OpenManage Network Manager only needs this additional data for an Alarm message, then this would be better configured as latent mining of variable bindings of the Alarm. Critical mining is configured through the `<MineVarBindObjects>` tag within `eventdefs.xml` files.
8	Entity lookup	By default, OpenManage Network Manager associates Events with the IP address of the device from which the original trap (or other kind of message) came. The entity lookup process associates the Event to a subcomponent or other type of entity if necessary based on the available variable bindings. Sometimes OpenManage Network Manager must configure Event definitions to associate Events based on them to the appropriate entities. You can configure these through the `<EntityLookup>` tag within `eventdefs.xml` files. See Entity Lookup on page 501 for details.
9	Resolve Notification Type OID from BED or EED	The notification type OID is set on the Event either from the matching base event definition (BED) or if there is an extended event definition (EED) whose extension bindings match those in the Event then this notification type OID is used instead. All default properties (such as severity, behavior, etc.) and EPRs associated with the resolved Event Definition are used, whether this happens to be a BED or EED.
10	Normalize device-specific data for standardized Event processing	If the Event came from a device-specific trap then an Event Processing Rule of type Device Access may exist that can normalize the payload. This then facilitates standardized Event processing. For example, OpenManage Network Manager can convert an Event based on a Cisco-specific definition reporting on a failed login to a generic Event that still reports on the failed login, but is not Cisco-specific. OpenManage Network Manager applies any EPRs whose filter conditions match the incoming Event here.

Process	Description
11 Apply Event Definition override mappings	By default, the Event Definition determines the data attributes of an Event, but some Event Processing Rules can override these defaults. Such EPRs can override attributes like severity, service affecting, and behavior. OpenManage Network Manager applies any such enabled EPRs whose filter conditions match the incoming Event here.
12 Apply stream base correlation	OpenManage Network Manager considers frequent Events a stream that might correlate within the steam base. Users can control stream base correlation by creating Event Processing Rules to detect patterns in the frequency of incoming Events for the purpose of minimizing the number of Events submitted to the application server for further processing. This includes EPRs of type State Flutter and Frequency Threshold. OpenManage Network Manager applies any such enabled EPRs whose filter conditions matches the incoming Event here. If an Event matches a steam base correlator then this step might be the end of its processing.
13 Marked for reject?	Is the behavior of the Event "Reject"? If so, then OpenManage Network Manager does insert it into the database. In most cases rejected Events do not go to the application server for further processing if, but some Events require a trigger for correct system behavior and therefore must be processed by the system even when rejected. OpenManage Network Manager posts such Events to the application server for further processing but does not insert them into the database.
14 Reject	OpenManage Network Manager rejects the Event rather than inserting it into the database. Note that even rejected Events might have some effect, like triggering device driver processing, despite not being persisted to the database. See # 13. *Marked for reject?*
15 Post Events to application server	In distributed environments, much of this processing is going on within the mediation server. Events that make it through to this point are posted to the application server so that they can be inserted into the database and for additional processing to take place that depends on data that needs to be queried from the database, including Alarm Correlation.
16 Receive Events	Application server receives Events from the mediation server.
17 Execute device driver processing	Some managed devices have drivers that feature follow-up Event processing. If the Event originated from a such a device then this step executes that follow-up processing.
18 Perform Alarm Correlation	Go to step one of the Understanding Alarm Life Cycle diagram. This process might create, edit, or clear an Alarm.
19 Persist Event to DB	Saves the Event to the database for future reference.
20 Execute automation actions	If any automation Event Processing Rules satisfy the filter conditions of the Event, then the OpenManage Network Manager application executes the associated actions here. Actions may include sending an email, forwarding the Event northbound as an SNMP trap, signifying that the configuration was changed on the device, and so on.
21 Done	Processing on the application server is done for this Event.
22 Apply Database Aging Policy	This begins the process that applies Database Aging Policies (DAP) to delete old Events.
23 Delete old Events	Delete the old Events according to the active DAP for Events.
24 Done	Done applying database aging policies for Events.

Understanding Alarm Life Cycle

The following diagram shows the OpenManage Network Manager alarm processing flow.



The following items correspond to the numbered processes in the diagram.

Process		Description
1	Alarm correlation	An Event occurred and was not marked as *Reject*.
2	Marked as suppress?	Is the behavior of the Event Suppress? At this point, this might occur because of the default behavior of the Event Definition or possibly because of an override mapping event processing rules (EPR).
3	Event is persisted but creates no Alarm	If OpenManage Network Manager suppresses the Event then it is inserted to the database but the insertion creates no Alarm
4	Source entity under Alarm suppression?	Is the entity that is the source of the Event under Alarm suppression? This can be scheduled or indefinite.
5	Severity is already set to cleared	Is the severity of the Event set to Cleared?
6	Clear open correlated Alarms	Clear all open Alarms correlated to this Event. Correlated implies more than one meaning for Alarms and/or Events: this correlation refers to rising/clearing correlation. How the Event Definitions associated with these Alarms/Events are correlated to each other is what drives this.
7	Latent mining of variable bindings	OpenManage Network Manager must sometimes return to the device that sent the original trap to "mine" additional variable bindings. Such mining can be either critical or latent, depending on whether this additional information is needed early in the Event life cycle or whether it can wait until after OpenManage Network Manager creates an Alarm. If OpenManage Network Manager needs additional data to associate an Event to an entity (which happens in # 8. Entity lookup in the Understanding Event Life Cycle diagram) then mining is critical, as described below. Critical mining of variable bindings also within the Event Life cycle diagram. On the other hand if this additional data is only needed to for an alarm message, then it this would be better configured as latent. This drives off the <MineVarBindObjects> tag of the bindobjectdefs.xml files.
8	Opened correlated Alarms exist?	Are there any open Alarms that correlate to this Event? Here, "correlated" refers to the correlation of a single open Alarm to one or more Events. The first of these was the Event that made the Alarm open. If the original Alarm is still open, each subsequent correlated Event does not open a new Alarm, instead incrementing this Alarm's count. Events correlate to existing open Alarms provided it meets all of the following conditions: 1) It is based on the same Event Definition as the Alarm 2) It has the same values for all key bindings as the Alarm 3) It is associated with the same entity as the Alarm.
9	Correlated Alarm has the same severity and message?	Are the severity and the message associated with this new Event the same as those of the correlated Alarm?
10	Escalate/de-escalate to new severity and message	Escalate or de-escalate the correlated Alarm by editing its severity and message to match that of the new Event.
11	Increment Alarm count	Increment the count of the correlated Alarm.
12	Clear extra correlated Alarms	Only one open correlated Alarm can exist. It is unusual, although not impossible, for more than one open Alarm to correlate to each other. If this happens it would probably be due to concurrency issues across multiple application servers. If this does happen then one of the Alarms can stay open and OpenManage Network Manager clears the others.

Process	Description
13 Open new Alarm and persist to DB	Open a new Alarm and persist it to the database so that it can be queried later.
14 Perform automatic parent/child correlation	If your configuration designates open Alarms the parent or child of a new Alarm then OpenManage Network Manager automatically creates the parent/child relationship. This derives from configurations made within the Event Definitions that are the basis of the Alarms. You configure this through the *CorrelatedParentData* tag of the eventdefs.xml files.
15 Alarm Propagation	This is the start of process propagating Alarm States to associated entities.
16 Propagate up and/or down the resource hierarchy	Depending on the Alarm's resource propagation attribute, it might propagate Alarm States to the subcomponents of the alarmed entity and/or to the top level device.
17 Propagate to associated Links	Propagate the Alarm States to the Links associated with the source entity. OpenManage Network Manager compares the severity of the A and Z endpoints and sets the severity of the Link to the higher of the two.
18 Service affecting?	Is this Alarm service affecting? This will either come from the default behavior of the Event Definition or else a mapping Event Processing Rule (EPR) may override it.
19 Propagate Alarm State to deployed Services and Customers	Propagate the Alarm State to the deployed Services and Customers associated with the source entity. This uses the severity calculator configured for the association type being used to route the propagation. This occurs one association route at a time, where if one routing and calculation results in a change in severity of the target entity then it will find the targets associated with that entity and route to them to do another round of calculation. This propagation is recursive and only stops once there are no more target entities whose severity has changed as a result of the calculation.
20 Done	Processing on the application server is done for this Alarm.
21 Clear Alarm request	The user manually clears an Alarm.
22 Persist clear to the database	The database is updated to make this Alarm cleared.
23 Execute Propagation	Go to # 15. Propagate Alarm States to the associated entities.
24 Alarm has children?	Does the Alarm have children? This includes other Alarms that are caused by or blocked by this one.
25 Clear child Alarms	Clear all of this Alarm's children.
26 Un-parent child Alarms	Update all of this Alarm's children so that they are top-level Alarms (no longer children of any other Alarm).
27 Children are caused by parents?	Are the child Alarms caused by the parent? This comes from the correlation state of the child Alarms. There is more than one sense of what it means for Alarms and/or Events to be "correlated" so to clarify in this context the "correlation state" refers to Alarm parent/child correlation.
28 Done	Processing on the application server is done for this Alarm.
29 Apply Database Aging Policy	This is the start of the process that applies Database Aging Policies (DAP) to delete old Alarms.
30 Delete old Alarms	Delete the old Alarms according to the active DAPs for Alarms. Note that there can be more than one active DAP, which might include one to delete old cleared Alarms and possibly another to delete very old Alarms that are still open, if this is desired.
31 Done	Done applying database aging policies for Alarms.

4

Generating Reports

This section provides the following tasks related to creating a report template, generating reports, and printing groups of reports:

Creating a Report Template – 130
Generating a Report – 131
Branding Reports – 132
Adding Custom Report Images – 132
Printing Groups of Reports – 133
Example Reports – 134

Creating a Report Template

Formatting counts in making reports useful. Sometimes the output limitations need to inform the formatting you select. For example, PDF output does not handle large numbers of columns well, while CSV (importable into Excel) output has no problem with it. Best practice is to test reports you configure before putting them into production. For a detailed description of the Report Templates portlet and related editors, see Report Templates Portlet on page 618.

Create a report template from the Report Templates portlet as follows.

1. Right-click the portlet and then select New > *templateType*.

   The Creating New Report Template window is displayed.

2. Name the template (for example: Test Amigopod Report).
3. Optionally enter a detailed description for the template.
4. Make sure that the advanced settings are correct, such as orientation.

   The defaults are Landscape.

5. Click the Source tab.

   The Source panel displays a list of inventory sources.

6. Select an inventory source (for example: Inventory resources [A - DD] Amigopod).

   A list of values related to the selected source is displayed.

7. Select the appropriate value.

   The Inventory columns lists are populated.

8. Select a type.
9. Populate the selected columns list from the available columns list (for example: Amigopod: Administrative State, Amigopod: DNS Hostname, Amigopod: Equipment Name, Amigopod:IP Address)

   If you populate the selected columns list in the order you want them to appear in the report, they automatically appear in this order on the Layout panel and you can skip to step 12. Otherwise, continue with step 10.

10. Click the *Layout* tab.

    The Layout panel lists the column order (top is first, bottom is last) and the default column settings.

11. Click the Edit action tool to modify a column's the font size, color, alignment, and so on and then Apply your changes.
12. Click *Save*.

    You have successfully created a template.

Generating a Report

To generate a report, you first configure the report and then generate it from the Reports portlet. For a detailed description of the Reports portlet and related editors, see Reports Portlet on page 612.

NOTE:

If you create a report based on interface monitoring, remember, the interface monitor is disabled as default. Additionally, some reports rely on data collected through Actions and are empty unless the Action supplying data is executed first. For example, to generate a report using VLAN data, you need to execute the "Get VLAN Data" action first. Without data, the report is empty.

For an example of a standard system report, see User Login Report on page 135.

Generate a report from the Reports portlet as follows.

1. Right-click a report and then select New.

   The Creating New Report window is displayed.

2. Name the report (for example: Test Juniper Router Report).
3. Enter a title and/or subtitle for the report (such as Juniper Routers).
4. Select a template for the report.

   For example, the template configured in Creating a Report Template on page 130.

   Note that if you create a template, the first report you create after making that template automatically selects the newly created template.

5. Click the Filters tab.
6. Add a a filter to confine the reports input to certain devices, locations, and so on.

   For example, select the existing All Juniper Routers filter.

7. Click Save.
8. Locate the newly created report in the Reports portlet.
9. Right-click the report and then select Execute Report.

   A message of success or failure is displayed.

10. Click My Alerts from the portal status bar.

    The My Alert/Action History window displays a notification that the report is ready for viewing.

11. Click the magnifying glass tool for the report message.

    The report displays in a new window.

12. Hover your cursor over the lower right corner of the report to show tools that let you expand, zoom out and in, save, or print the report.

Branding Reports

Reports come with a default logo, but you can change that. Put the graphic file (.png, .jpg or .gif) with your desired logo in a directory on the application server.

△ CAUTION:
If you have a distributed installation, make sure this image and property are on all servers.

Brand reports with a different logo as follows.

1 Create an image that is no taller that 50 pixels, and no wider than 50 pixels.

2 Save the image file as .png, .jpg, or .gif.

3 Navigate to the installed.properties file located in the owareapps/installprops/lib/ directory.

4 Alter the image property in the installed.properties file.

```
redcell.report.branding.image=<filename_here>
```

For example:

```
redcell.report.branding.image=C:/installPath/owareapps/redcell/images/
    TestImage.png
```

Notice that you **must** use the forward slashes, (not backslashes as is typical of Windows) when you specify the path.

5 Verify that the logo changes by generating a report.

Adding Custom Report Images

You can uploading images that appear, branding reports into the portal's Documents and Media portlet. Put them in the pre-seeded folder named *Report Images*. By default reports use the site logo in reports if you have set up no override.

Site Override—To override the logo for every report that does not have an individual custom logo setup, upload the image into the Documents and Media/Reports Images folder and name it report logo. This image becomes the site's default report logo.

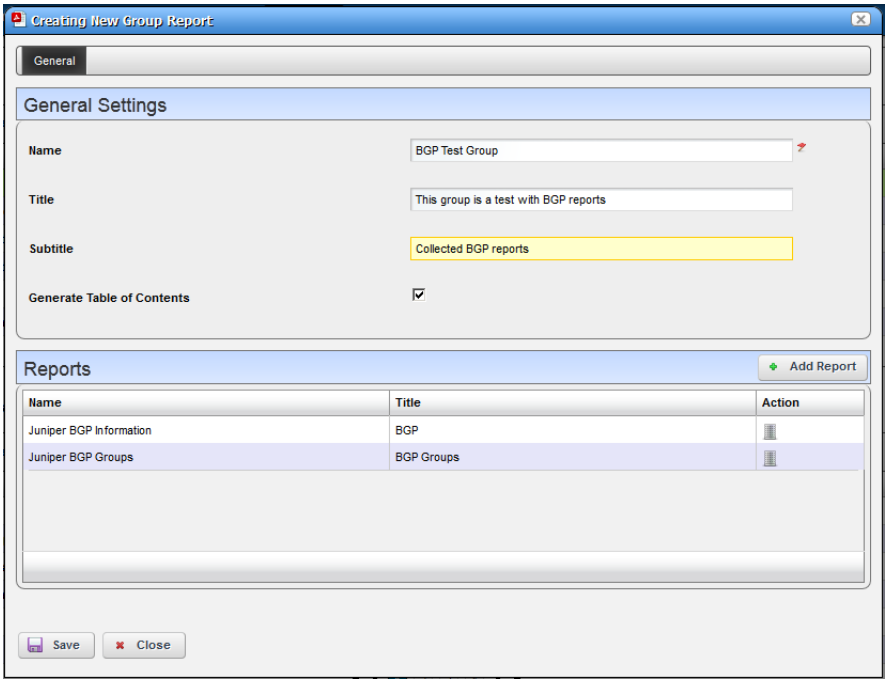
Individual Report Override—Individual reports. To override the logo for individual reports, upload an image into the Documents and Media/ Reports Images folder. It then appears in the report editor as a selectable branding images. Users can view and select these images if they have the correct permission with write privileges (Permission-RP:ReportTitleImage).

Printing Groups of Reports

You can print a collection of several reports and generate a table of contents if the collection is large enough to warrant it. Print groups of reports from the Reports portlet as follows.

1 Right-click and then select New Group.

The Group Report editor is displayed.



2 Enter the name and optionally a title and subtitle.

NOTE:

Reports within the report group are sorted by title. If no title specified, the report name is used as the map key.

3 Select whether to generate a table of contents.

4 Click Add Report (+).

A list of reports from which to select is displayed.

5 Select all that apply.

6 Click Add Selection.

7 Click Done.

8 Click Save.

Example Reports

This section provides the following example reports:

- Cisco Port Groups
- User Login Report
- Network Assessor Reports

Cisco Port Groups

The Cisco Port Group Report collects data on port groups and assembles that to display the current total bandwidth for port groups under a device or card.

This supports two types of port groups, both with 8 ports:

- One type is alternating groups of 8, so on a 48 port card, 1-8 would be one port group, 9-16 would be a second, 17-25 would be a third, and so on.
- The other type is even/odd alternating groups of 8, so on a 48 port card, ports 1, 3, 5, 7, 9, 11, 13, and 15 would be one group, while ports 2, 4, 6, 8, 10, 12, 14 and 16 would be a second group, 17, 19, 21, 23, 25, 27, 29, 31 would be a third group, and so on.

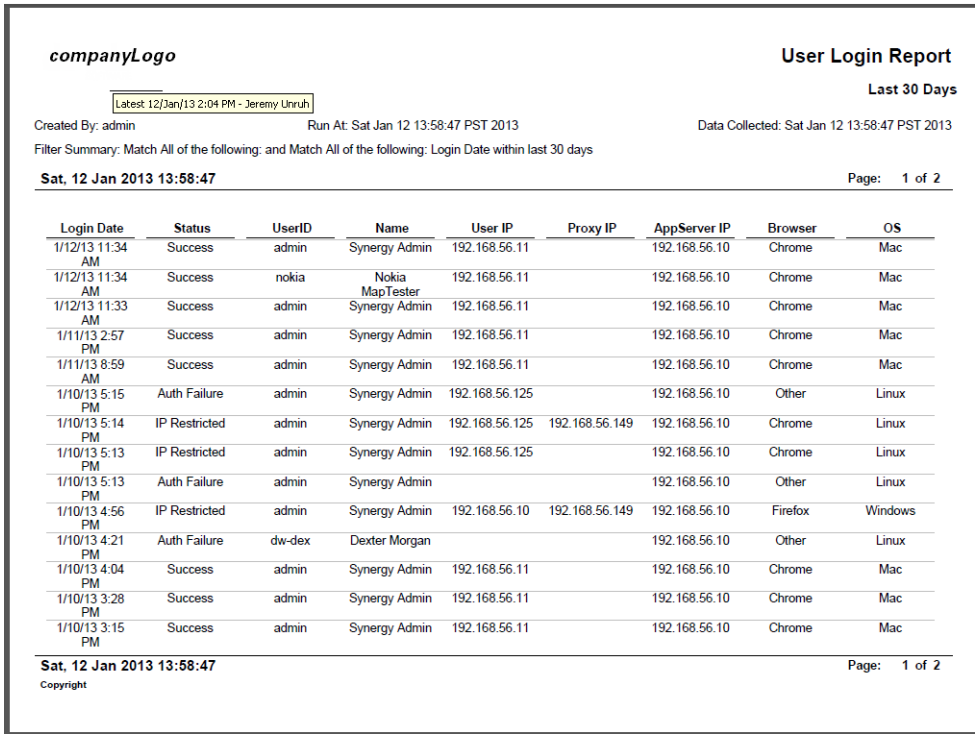
The following two properties in the owareapps/cisco/lib/cisco.properties file configure port collection:

```
com.dorado.cisco.portgroups.blockcards
com.dorado.cisco.portgroups.evensoddscards
```

Tou must add any card for which you want to gather port group data to one of these two lists, depending on what kind of port groups it wants to collect. Add the card by adding its MODEL NAME (example: WS-X6248-RJ-45). Delimit multiple models with commas. Examples are in the cisco.properties file comments.

User Login Report

In addition to reports about inventory, devices, and so on, the OpenManage Network Manager application lets you create a report documenting user logins.



companyLogo

User Login Report

Last 30 Days

Latest 12/Jan/13 2:04 PM - Jeremy Unruh

Created By: admin Run At: Sat Jan 12 13:58:47 PST 2013 Data Collected: Sat Jan 12 13:58:47 PST 2013

Filter Summary: Match All of the following: and Match All of the following: Login Date within last 30 days

Sat, 12 Jan 2013 13:58:47 Page: 1 of 2

Login Date	Status	UserID	Name	User IP	Proxy IP	AppServer IP	Browser	OS
1/12/13 11:34 AM	Success	admin	Synergy Admin	192.168.56.11		192.168.56.10	Chrome	Mac
1/12/13 11:34 AM	Success	nokia	Nokia MapTester	192.168.56.11		192.168.56.10	Chrome	Mac
1/12/13 11:33 AM	Success	admin	Synergy Admin	192.168.56.11		192.168.56.10	Chrome	Mac
1/11/13 2:57 PM	Success	admin	Synergy Admin	192.168.56.11		192.168.56.10	Chrome	Mac
1/11/13 8:59 AM	Success	admin	Synergy Admin	192.168.56.11		192.168.56.10	Chrome	Mac
1/10/13 5:15 PM	Auth Failure	admin	Synergy Admin	192.168.56.125		192.168.56.10	Other	Linux
1/10/13 5:14 PM	IP Restricted	admin	Synergy Admin	192.168.56.125	192.168.56.149	192.168.56.10	Chrome	Linux
1/10/13 5:13 PM	IP Restricted	admin	Synergy Admin	192.168.56.125		192.168.56.10	Chrome	Linux
1/10/13 5:13 PM	Auth Failure	admin	Synergy Admin			192.168.56.10	Other	Linux
1/10/13 4:56 PM	IP Restricted	admin	Synergy Admin	192.168.56.10	192.168.56.149	192.168.56.10	Firefox	Windows
1/10/13 4:21 PM	Auth Failure	dw-dex	Dexter Morgan			192.168.56.10	Other	Linux
1/10/13 4:04 PM	Success	admin	Synergy Admin	192.168.56.11		192.168.56.10	Chrome	Mac
1/10/13 3:28 PM	Success	admin	Synergy Admin	192.168.56.11		192.168.56.10	Chrome	Mac
1/10/13 3:15 PM	Success	admin	Synergy Admin	192.168.56.11		192.168.56.10	Chrome	Mac

Sat, 12 Jan 2013 13:58:47 Page: 1 of 2

Copyright

This report can include the following attributes: Login Date, Status [SUCCESS, AUTH FAILURE, IP RESTRICTION], UserID, User Name, User IP, Proxy IP (if going through a Load Balancer/ Proxy), AppServer IP, Browser [CHROME, FIREFOX, and so on], Operating System [WINDOWS, LINUX, MAC, IPHONE, IPAD, and so on.]

The following attributes are available, but not in the default seeded report to conserve Column space: Portal IP and Browser Version.

When authentication fails, this report does not record the IP address from which the user made the attempt, unless such users are behind a proxy or load balancer.

Browser ID, Version and Client appear only by best effort. Browsers do not always send the user-agent and can change standard messaging with extra plugins.

NOTICE

A Default User Sign-On Log DAP exists, which by default keeps the last 30 days.

Network Assessor Reports

If you have the Network Assessor option (assessor.ocp) installed, it includes reports like the following: *Asset Report ALL Resources*, *Software Version Report*, *IP - Hostname Only Report*, *IP - Hostname Report*, *Configuration Change Report*, *Hardware Change Report*, *Software Change Report*, *NetConfig Backup Status Report*, *NetConfig Deploy Status Report*, *NetConfig Restore Status Report*, *Card Report*, *Firmware Report*, *Interfaces Report*, *Inventory Report*, *Port Report*, *Primary Contact Report*, *Subnet Report*. You can also see an *EOL Report ALL Devices* (EOL means "End of Life").

The *EOL Report ALL Devices* report tells which of your discovered equipment has passed its end of life or end of service. A registration script (RegisterEOL) in the **.../owareapps/assessor/bin** directory registers EOL information different from the defaults that ship with the Network Assessor option. To update your EOL/EOS ("End of Life"/"End of Service") dates, create a text file (myEOL.txt) with EOL and EOS definitions as a parameter for RegisterEOL. Construct this parameter file as follows:

EOL=SysobjectID, EOL True False, EOL Date (mm/dd/yyyy), EOS True False, EOS Date (mm/dd/yyyy)

Here is an EOL and EOS example text file:

```
# Example (below) Cisco AS5200 Series Universal Access Servers AS5200,,,,
EOL=1.3.6.1.4.1.9.1.109,True,07/14/1999,True,07/23/2010
```

where:

1.3.6.1.4.1.9.1.109 is the SysobjectID for a Cisco AS5200 Universal Access Server . Remember to preceed the objectID with EOL=

True sets the End Of Life indicator to true

07/14/1999 is the End Of Life date

True sets the End of Service indicator to true

07/23/2010 is the End of Service date

Once you created your EOL/EOFS text file (myEOL.txt), follow these steps to register the file.

1. Save the myEOL.txt file to *installDir*/owareapps/assessor/bin directory.
2. Navigate to *installDir*/owareapps/assessor/bin directory.
3. Execute the RegisterEOL script while the server is running.
   - In Linux, run these commands:
     ```
     . /etc/.dsienv
     ./RegisterEOL myEOL.txt
     ```
   - In Windows, run these commands:
     ```
     oware
     RegisterEOL myEOL.txt
     ```

   The "New EOL Definition was processed" message is displayed.

5

Managing Resources

The Resource management portlets let you manage devices you have discovered or created on your network and iew device-specific information, both general (name, type, location, contact) and technical (vendor, subcomponents, and so on). For a detailed description of the resource management portlets, see the following OpenManage Network Manager User Interface on page 441 sections:

- Authentications Portlet
- Discovery Profiles Portlet
- Managed Resources
- Ports Portlet
- Report Templates Portlet
- Reports Portlet

NOTE:

Your software may come with pre-seeded Authentications and Discovery Profiles examples so you can see what they look like.

This section provides the following resource management tasks:

Discovering Resources – 138
Modifying Discovery Profiles – 139
Logging Terminal Sessions – 140
Setting Java Security for Terminal Access – 141
Changing Customer to Port Associations – 141
Using the Add Ports Action – 141

Optional applications and device drivers may increase the basic functionality described here, your steps my differ slightly from the example steps provided.

Discovering Resources

This section outlines some basic resource discovery steps. Discover resources as follows.

1 Set up Authentications for the resource you want to discover.

   a. Click Settings from the navigation bar.

   b. Right-click the Authentications portlet and then select New.

   c. Enter a unique identification.

   d. Add any associated equipment.

   OpenManage Network Manager must be authorized to set CLI session parameters; permissions-related timeouts may occur during device access if it is not enabled. For example, Cisco CLI access requires the `set terminal length 0` command.

2 Set up the Discovery Profiles for the resource you want to discover.

   a. Select Resources > Discovery from the navigations bar.

   b. Right-click the Discovery Profiles portlet and then select New.

   c. Enter a unique name for the profile.

   d. Specify the discovery, network, actions, and inspection options.

   e. Execute the profile.

      If the discovery fail, use the Network Tools Portlet on page 549 to confirm that any device missing from discovery is online. The device itself must permit the OpenManage Network Manager system access it.

3 View the results in the Managed Resources portlet.

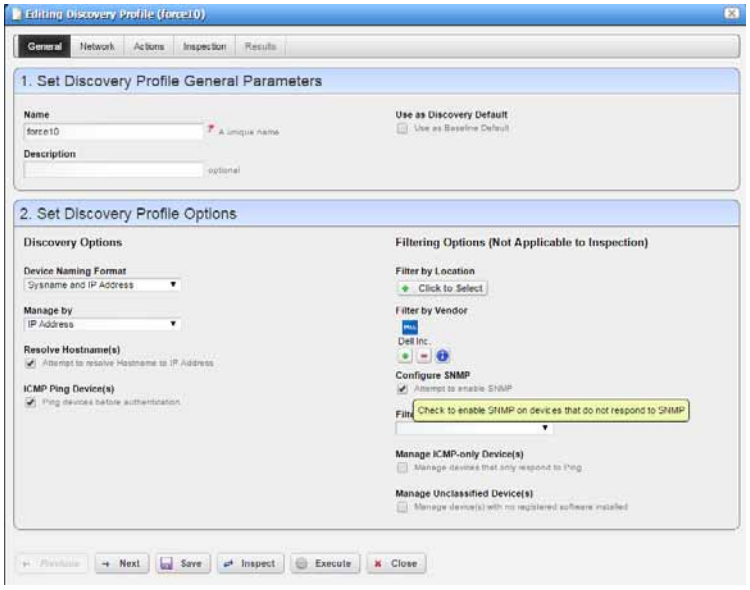
Modifying Discovery Profiles

Modify discovery profiles from the Descovery Profiles portlet as follows.

1 Right-click the profile you want to modify.

2 Select Edit.

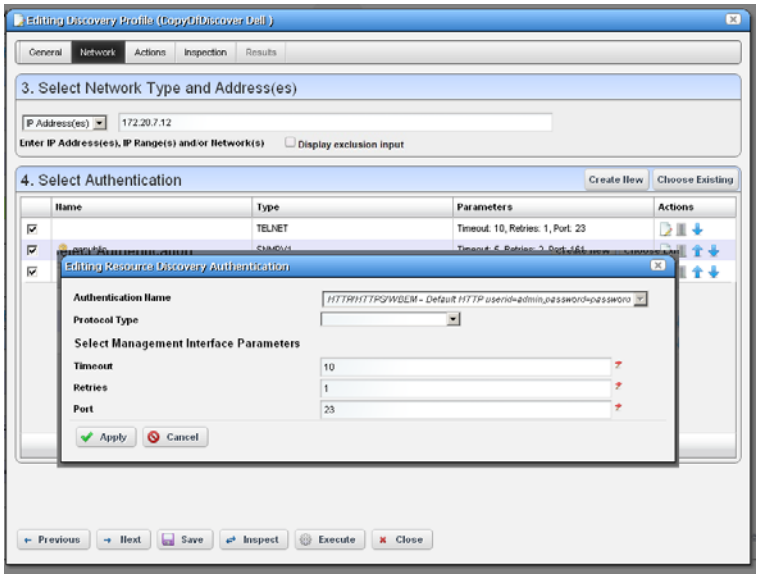
The Discovery Profile editor is displayed.



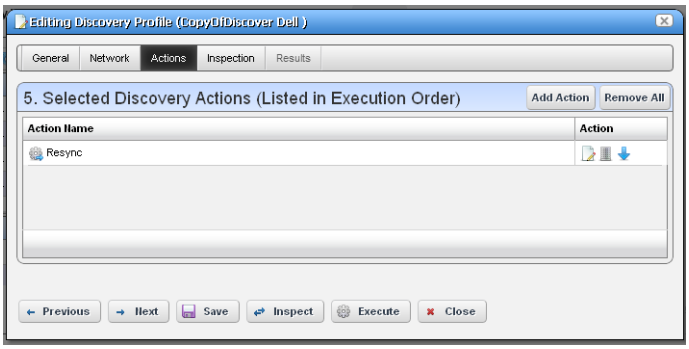
3 Modify the general parameters and profile options as needed.

4 Click the Network tab and then modify network types or authentication.

The Network panel is displayed.



5 Click the Actions tab and then modify actions as needed.



6 Click the Inspection tab and then modify settings as needed.

7 Click Save to preserve the profile.

If you execute the profile before saving it, the OMNM system does not save the profile to execute later.

8 Click Execute.

The Results panel displays the message traffic between the OMNM system and the device. When processing completes, Success or Failed is displaye. The portal also displays a successful completion, unable to execute, or failed message.

9 Close the Discovery Profile editor.

Logging Terminal Sessions

Log terminal sessions (if you like) as follows.

1 Enable Java Console on the client.

- For Windows, do this in Control Panel.
- On Linux you must navigate to the install location of your JRE and run the Console script. Select the Advanced tab and change the Java Console setting to show the console.

  Java Control Panel > General tab > Settings displays the location where the logs are stored.

2 Open a *Direct Access* > *Terminal* session by right-clicking a device.

The Java Console appears.

3 Configure the logging level in the *Terminal* menu of the direct access screen.

Levels, in increasing order of detail, include *None*, *Info, Debug,* and *Trace*, which echoes keystrokes.

Setting Java Security for Terminal Access

Newer Java distributions (7+) block websites with self-signed certificates, which interferes with Direct Access. You need to provide a security exception for the OpenManage Network Manager (OMNM) application server to avoid issues.

Set Java security for terminal access as follows.

1. Access the Java control panel by doing one of the following:
   - From Windows, locate the `configure java` program and open it.
   - From Linux, locate the JRE installed and associated to your browser and then run the `../jre/bin/ControlPanel` script.
2. Select the *Security* tab and then click *Edit Site List*.
3. Click Add.
4. Enter the OMNM URL (example: http://192.168.0.51:8080/).
5. Click OK and Continue.
6. Apply this change and/or click OK.

   Direct access functions correctly after you make this adjustment.

Changing Customer to Port Associations

You can associate or dis-associate a customer with a port or interface using the Associate Contact to Equipment or Remove Associated Contacts actions.

Change customer port associations as follows.

1. Execute the action (Associate Contact to Equipment or Remove Associated Contacts).
2. Select the port and contact.
3. Finish executing the action.

Using the Add Ports Action

A Manage-type Action lets you add Juniper device ports to the OpenManage Network Manager (OMNM) database before resync picks them up. These can be ports created by Adaptive CLI actions that simply add ports without updating the database, or those added outside the OMNM application. Once ports are in the database, you can then use them in services in in the Service Center. The advantage of having this action available explicitly is that you do not have to wait for a resync to populate the database correctly.

△ CAUTION:
This Management Action works only for ports already added to the device. Using it to add to the OMNM inventory first then running automated or manual resync removes the port from the database.

Use the Add ports action from the Managed Resources portlet as follows.

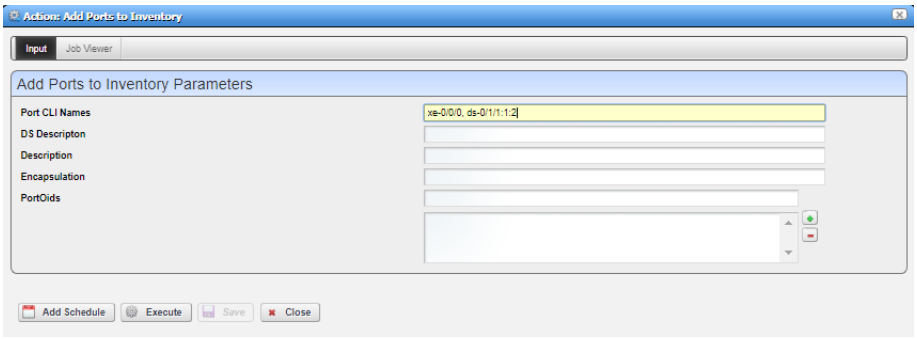
1. Right-click a device and then select Actions.

   The Actions Selection window is displayed.
2. Click the Manage tab.

3 Select Add Ports to Inventory > Continue.

The Action editor displays the input parameters.

4 Enter the CLI names of one or more ports to add (separate multiple entries with commas).



5 Execute or schedule the Action.

If you enter something not in a format like a port (xx-#/#/#, or xx-#/#/#:#, and so on), the OMNM application does not attempt to add it. If you enter a port identifier for which the OMNM application cannot find, the OMNM application does not add the port. For example, the parent card (ge-1/10/20) when no card with a containerIndex 1, slotNumber 20 is in the database.

The OMNM application does not populate any of the details other than name, CLI name, slot number, and icon. The OMNM application retrieves any other attributes when a normal resync occurs.

6

Using Visualization Tools

You can display devices and network arrangements in a variety of ways. The following sections describe those display strategies.

Understanding Containers – 144
Using Containers – 145
Setting Up Google Maps – 145
Setting Up Nokia Maps – 146
Creating a Topology View – 147
Modifying Visualize Label Length – 147
Exporting to Visio – 148

Understanding Containers

Containers manage what appears in other portlets on the same page, including Visualize and Maps portlets. If a page with a Visualize portlet has no Container View portlet, clicking a visualize node limits other portlets on that page to only that node's information (for example Alarms).

Here are the **context display rules** for how portlets manage each others' displays:

Rule	Description
1	If the Container View portlet is on a page, its selections drive all portlets that accept context. If you have no containers configured, the other portlets are empty. If the Container View portlet is not on a page, then the remaining rules may apply.
2	If the Visualize My Network portlet is on a page, it acts like the Container View portlet and drives all portlets' appearance.
3	If rules 1 and 2 **are not** in effect, the Managed Resources portlet drives Ports and Links portlets' appearance.
4	If rule 1 **is not** in effect and the Visualizer Views portlet is on the same page as the Visualize My Network portlet, the selected view appears in the Visualizer.

The context rule displays in a portlet's header if its appearance is being managed by another portlet as defined by these context display rules.

When a page with a container loads, the container loads first and then starts polling. If a visualizer is on the same page as a container, the visualizer starts its polling after the page loads, so some lag may occur between the Container View and Visualizer Views portlets, depending on your settings. Clicking Context from a portlet or drilling down or expanding nodes in the Visualize view resets the refresh timer since it may poll different nodes. This can also offset refresh timing for different page elements. You can change refresh timing from the Application Settings window (see Redcell > Application Settings on page 686 for details), but synchronizing such portlets is not likely.

NOTE:

Some portlets may display a selected context without operating as though it was selected. For example if you put Managed Resources.

Some pages **may not** exhibit this default behavior. For example, custom branding on pages may interfere with these rules, in which case, you can see the default behavior by creating a new page with the relevant portlets. You may also try refreshing the page.

You can disable the context responses in the Alarms portlet in its preferences menu (click the wrench). When you disable context responses, the Alarm portlet instance's auto refresh displays new, unique alarms, but does not display, for example, a selected container's alarms. Otherwise, you must change the context call from the Container View to refresh alarms.

Using Containers

Use containers as follows.

1 Create the containers you would like for filtering resource views.

For example, create a container for each customer or location.

CAUTION:
By default containers are configured without any authorizations. Make sure that you configure authorizations so you can see the container once it is configured. Otherwise, it is not visible.

a. Navigate to the Container Manager portlet (Alarms > Alarms by Container).

b. Right-click the portlet and then select New.

The Creating New Root Container window is displayed.

c. Enter a name and description.

d. Specify membership, such as customers.

e. Set Authorizations.

f. Choose the visualizer display object.

g. Click Save.

2 Create a page with the Managed Resources portlet or other container-filtered portlets (Ports, Alarms, and so on).

3 Add the Container View portlet to that page.

4 Select the container to filter by.

5 Observe the other portlets to see resources assigned to the selected container, such as, customer or location.

Setting Up Google Maps

Google now requires an API key to use their google maps API. Set up Google Maps as follows.

NOTE:
If you do not specify an API key, the OpenManage Network Manager (OMNM) default key is used but you may be severely limited in the number of map downloads you can make.

1 Go to https://console.developers.google.com.

2 Create a google account if you do not already have one.

3 Click the APIs & Services Library link.

4 Click Google Maps JavaScript API.

5 Click Create Project.

6 Click Create a Project under API Manager Dashboard.

7 Type in a project name and click yes to agree to terms of service.

8 Click Create.

9 Click Enable.

10 Click Create Credentials.

11 Under “Which API are you using?” select “Google Maps JavaScript API”.

12 Under “Where will you be calling the API from?” select Web browser (Javascript).
13 Click the “What Credentials do I need?” link.
14 Type a name for your API key.
15 Click Create API key.
16 Copy down the API key value.
17 Go to the OMNM Control Panel > Redcell >Application Settings.
18 Click the User Interface tab.
19 Select Google Maps as the map provider.
20 Enter the API key in the Application ID field.
21 Click Save.

Setting Up Nokia Maps

UsingNokiaMaps

By default, the OpenManage Network Manager (OMNM) application uses Google maps. To use the Nokia maps service, you need App ID and App token. Set up Nokia maps service as follows.

1 Get an ID and token from https://developer.here.net.
2 Click Sign In.
3 Click on Register.
4 Create Your Nokia Account.
5 Click Register.
6 Click “Create app” and provide an application name.
   For example: OpenManage Network Manager
7 Click Get Started.
8 Click Done.
9 Copy the App ID and App token.
10 Go to the OMNM Control Panel > Redcell >Application Settings.
11 Click the User Interface tab.
12 Select Nokia Maps as the map provider.
13 Enter the API key in the Application ID field.
14 Click Save.

Creating a Topology View

Creating a topology map of devices or services is as simple as right-clicking the items you want to map, and selecting Visualize. You can also save different topologies after configuration and fine-tune its appearance using the tools provided. For a detailed description of the Virtualize portlet and its available options, see Visualize Portlet on page 517.

CAUTION:
If you installed a firewall on the application server, ports 80 and 8080 must be open for topology to work.

Create a topology map as follows.

1. Navigate to the Managed Resources portlet.
2. Select the items you want to include in the topology map.
3. Right-click the selections and then select Visualize.

   The Visualize portlet is displayed.

   Note that Topology uses Adobe Flash. The pop-up menu includes the Flash Settings, Global Settings, and About Flash menu items.
4. Organize the objects and draw the needed connectors.
5. Save your view.

   Your view is now available from the Visualizer Views portlet.
6. Fine-tune your view using the Overview, Layout, and Properties options.
7. Save any changes.

   If you do not see what you expect, make sure that you refresh your browser so cached images do not interfere with current images.

   If you want to initiate Actions on a node or its components, right-click the node, select Details, right-click the reference tree node/component, and then select Actions.

Modifying Visualize Label Length

Extending Visualize Label Length

Labels default to 13 characters, but you can extend them to a wider size by adding the following property to the *installDir*/oware/synergy/conf/server-overrides.properties file:

```
nodes.labels.extended.width=true
```

Otherwise, you can force an extended label with your Extension so it is automatic. Using your extension, you can do it within the `PortletProvider#getPortalProperties()` call.

For example:

```
public Properties getPortalProperties() {
   Properties props = new Properties();
   props.put("nodes.labels.extended.width", "true");
   return props;
}
```

NOTE:
This allows labels to be much longer but adds the possibility of text bleeding on top of other nodes.

Exporting to Visio

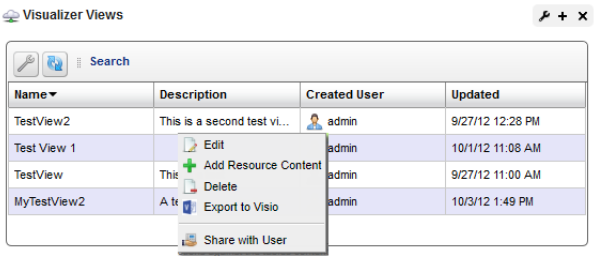
Export a topology view to Visio as follows.

1 Create a topology view if it does not already exist.

See Creating a Topology View on page 147 if you need some detailed steps.

2 Go to the Visualizer Views portlet.

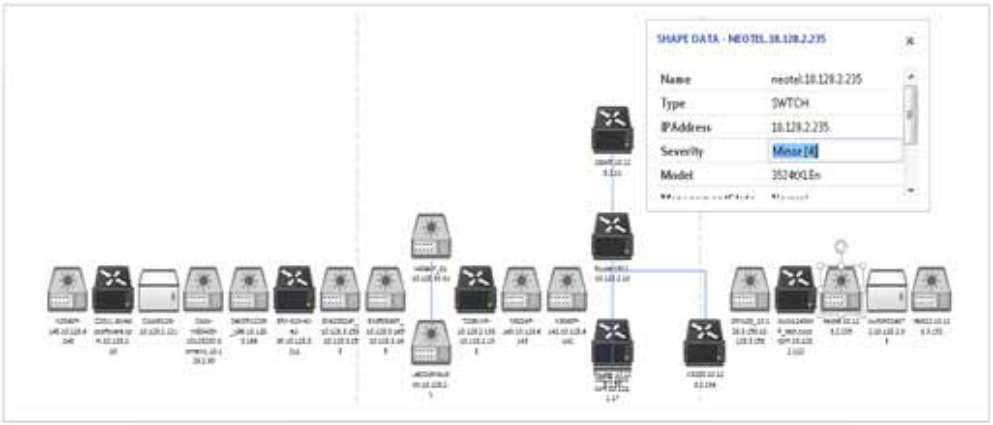
3 Right-click the view you want to export and then select Export to Visio.



A message displays indicating that the view was exported.

4 Click Download Visio File.

This downloads the Visio file to your browser. The equipment and link tooltips are saved in the Visio shape data. To see the shape data in Visio, right-click the shape or link (connector) and then select Data > Shape Data.



7

Managing File Servers/Files

This section provides the following tasks for managing your file servers and files:

Understanding FTP/TFTP Servers – 150
Backing Up Configurations – 151
Restoring Configurations – 152
Deploying Firmware – 154
Restoring a Configuration to Many Devices – 154
Creating/Comparing Promoted Configuration Templates – 155
Troubleshooting Backup, Restore or Deploy Issues – 156

Understanding FTP/TFTP Servers

Before you can push and pull configuration files to and from devices or deploy firmware updates, you need to configure FTP, TFTP, or both file servers.

CAUTION:

The internal FTP/TFTP server is for testing only, not for production use. Service discovery may not function correctly with the internal FTP/TFTP server. No internal server is available on Linux installations.

Port conflicts prevent an external file server and internal file server from operating on the same machine.

You need not be concerned that the internal server may provide insecure access to the OpenManage Network Manager (OMNM) application. The internal file server was designed to be ultra-secure. It creates a separate authentication and virtual file system for each file retrieved. It also only responds to OMNM internal requests.

NOTE:

The internal FTP server is primarily for testing, not production systems. It may not function in all cases. Configure an external file server and use it instead if and when the internal file server fails.

The following sections provide some more specific information related to FTP/TFTP servers:

- File Permissions
- Recommended Windows File Servers
- External File Server Editor

File Permissions

The OpenManage Network Manager (OMNM) application automatically deletes any temporary file created as part of an FTP/TFTP interaction. If the directory you selected for your servers does not have permissions needed to make these deletions, transactions still proceed. The OMNM application does print a warning saying the deletion failed, and the details panel suggests checking to make sure delete permissions exist in the relevant directory. Omitting such permissions causes no loss of functionality, but the server may fill up with the remnants of old transactions.

When you test a TFTP server on a Windows system, you may see the following error:

```
FTP umask / permissions of file on server are incorrect
```

This is an artifact of Windows permission structure, and may be safely ignored (test your TFTP server just to make sure).

NOTE:

For Linux TFTP servers, a typical configuration line in the /etc/xientd.d/tftp file is:

```
server_args = -c -p -u ftpuser -U 177 -s /home/ftpuser
```

Recommended Windows File Servers

Recommended Windows File Servers

The open source Filezilla server works as a service on Windows servers. Any login/password access to these servers goes in the File Server editor login/password fields. To support TFTP, try the Tftpd32 or Tftpd64 (for 32-bit or 64-bit machines) open source.

These servers must read/write from/to the same directory. Also, make sure that the directory offers open read/write/execute permissions so you can retrieve files put there temporarily, and delete them once the process is done with them.

External File Server Editor

From the File Servers portlet, access the External File Server editor to manage your file servers and files. See External File Server on page 594 for a detailed description of this editor.

NOTE:

Secure FTP connections (scp/sftp) often require SSH services be enabled on the devices addressed. Make sure that your system's server and sftp/scp file server can also access the devices with SSH

FTP servers typically must be on the same side of the firewall as the devices with which they communicate. If you have several such servers, the specified Net Mask also determines which server communicates with devices in which portion of the network.

The OpenManage Network Manager (OMNM) file server uses an internal, local LAN address (192.168.100.100 example). However, the routers with which it communicates often cannot communicate to such internal addresses. Therefor, an external/reachable address is necessary. You can know an IP address used by the OMNM application, and another External IP Address used by these devices. If you configure multiple file servers, the OMNM application selects the server with the Net Mask whose subnet is closest to the devices with which it communicates.

Backing Up Configurations

The OpenManage Network Manager (OMNM) application simplifies backing up devices so you can always have their configuration, even if the device file becomes corrupted or out-of-date.

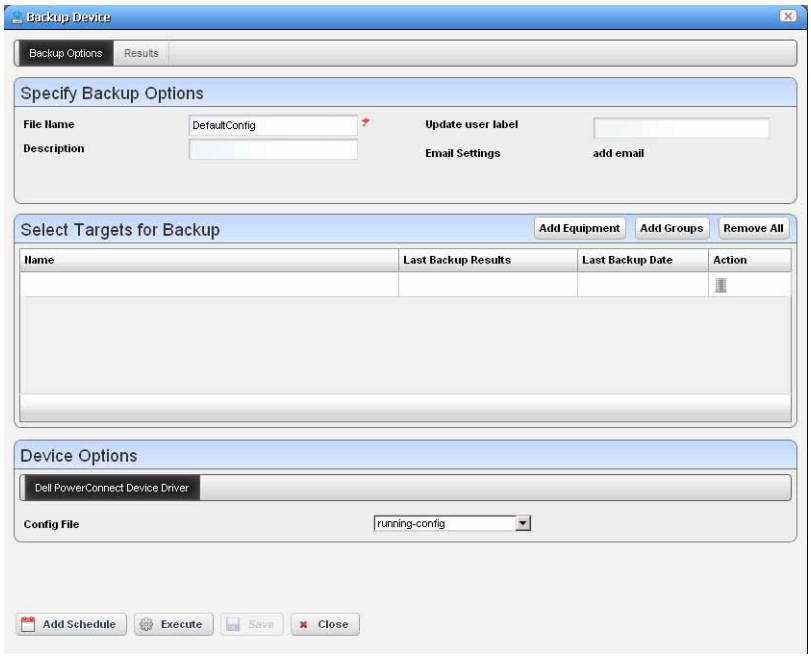
You can back up several devices at once. Use the standard Ctrl+click option in the expanded Managed Resources portlet to select several devices. Or, look for the appropriate group in the Managed Resource Groups portlet.

Back up your device configurations as follows.

1. Make sure that an FTP or TFTP server is configured to handle the backup. See File Servers on page 627.
2. Navigate to the Managed Resources portlet.
3. Right-click the devices and then select File Management > Backup.

   The Backup Device window is displayed.
4. Specify options, targets, and device options.

See Config File Backup on page 576 if you need a detailed description of these fields.



5 Execute the backup now. Otherwise, continue with step 6.

The Results panel displays the message traffic between the OMNM application and the devices. See Audit Trail Portlet on page 630.

6 Schedule the backup for a later time.

7 Click Save to preserve this scheduled configuration.

Restoring Configurations

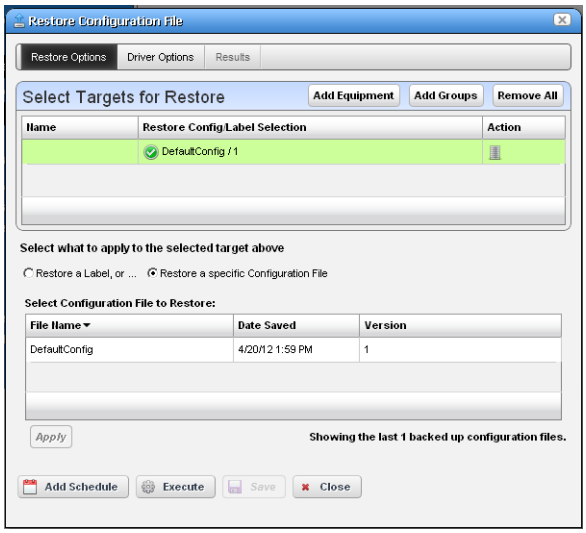
Restore a configuration file to a device as follows.

1 Make sure that an FTP or TFTP server is configured to handle the restore. See File Servers on page 627.

2 Navigate to the Managed Resources portlet.

3 Right-click the devices and then select File Management > Restore.

The Restory Device window is displayed. If you selected multiple devices, select a target from the list before continuing with the next step.



4 Modify the Targets for Restore list as necessary by:

This screen's tabs lets you configure the following:

- Deleting a target
- Adding equipment
- Adding groups

5 Select a target for restore.

6 Set and apply the restore options for the selected target.

This panel lets you select either a label (like *Current*, *Compliant* and so on—a selector listing available labels appears onscreen once you click this option), or *Restore a specific Configuration File*. The latter lists available files and lets you click to select.

7 Select the driver options for the selected target.

The Driver Options tab lets you select device-specific restoration options. If you are restoring to a group or multi-selected devices, as many tabs appear as are necessary to configure different restorations for different devices

8 Repeat steps 5 through 7 for each target listed.

9 Execute the backup now. Otherwise, continue with step 10.

The Results panel displays the message traffic between the OMNM application and the devices. See Audit Trail Portlet on page 630.

10 Schedule the restore for a later time.

11 Click Save to preserve this scheduled configuration.

Deploying Firmware

Deploy a device firmware image as follows.

1. Make sure that an FTP or TFTP server is configured.

   See File Management Menu on page 582.

2. Navigate to the Managed Resources portlet.
3. Right-click the devices and then select File Management > Deploy.

   The Deploy Firmware window information based on the selected device.

4. Select the firmware image you want to deploy.

   The fields are populated based on your selection.

5. Select a transfer protocol.
6. Modify the targets as needed, such as deleting a target, adding equipment, or adding groups.

   What you can do is restricted to devices that match the deploy file's type.

   CAUTION:
   You can also select devices, then change the OS selection so a potential mismatch may occur. This *may* trigger deployment rejection by the device, but is not a recommended experiment.

7. Specify any device options available to fine-tune the deployment.

   The options available are vendor-specific.

8. Execute the backup now. Otherwise, continue with step 9.

   The Results panel displays the message traffic between the OMNM application and the devices. See Audit Trail Portlet on page 630.

9. Schedule the deployment for a later time.
10. Click Save to preserve this scheduled configuration.

Restoring a Configuration to Many Devices

You can restore a single configuration to many discovered devices without overwriting those devices' essential information. Restore a single configuration to many discovered devices as follows.

1. Back up a single device's configuration that is closest to the configuration you want to see.
2. Navigate to the File Management Menu portlet.
3. Right-click this backed up file in the File Management Menu portlet, and Promote it (so it eventually appears in the portlet).

   The Editor appears for the promoted configuration.

4. Name the file.
5. Configure a Target Filter if necessary from the editor's General Parameters panel to confine it to certain devices by default.
6. Select the Configuration tab.
7. Locate the parameters you want to preserve in discovered devices when you restore this file.

   This can include items like the device's DNS Hostname, IP Address, and so on. Delete the file's specifics and double-click to insert the Target Params in place of these variables.

8 Save the configuration.

9 Right-click and then select Deploy.

This deploys the configuration to the targets you select.

You can select Generate and save for configuration only if you simply want to deploy later, and save for now. Also, optionally name a Configuration File Label for the deployed files.

10 Select the devices, or groups of devices to which you want to deploy.

11 Click Save, Execute or Add Schedule depending on your desired outcome.

If you click Execute, confirm the action.

When OpenManage Network Manager deploys the configuration, it reads the Target Params from those discovered for each device, inserts them in the deployed config file, then restores the configuration, device by device, skipping any that do not pass the filter set up in step 4.

Creating/Comparing Promoted Configuration Templates

If you want to store "template" configurations you have promoted, and compare them to previous templates, here are the steps to do that.

1 Select a configuration file and promote it to be a template.

Suggestions: Settle on a naming convention for these, perhaps one that includes a date so you can easily find and compare templates from different dates. You can also create a label for such configurations by simply typing in the *Label for Configuration* field. This should make such configurations easy to retrieve, particularly in the expanded Configuration Files portlet.

2 Enter the needed variables.

3 Save the template.

4 Right-click to *Deploy* it.

5 Select a single target and make sure to check the *Generate and Save Configuration Only checkbox*.

6 *Execute*. Rather than deploying the file, this saves a copy of the file as it would be generated for the single target in the Configuration Files Portlet.

7 When you have more than one of these configurations, find the files and Ctrl + click to select a pair of them, then right-click to *Compare* them.

Troubleshooting Backup, Restore or Deploy Issues

Here are some steps to troubleshoot issues you man encounter during a backup, restore, or deploy action. The following example steps are for troubleshooting a backup, but the steps apply to a restore or deploy action too.

1 Make sure the FTP / TFTP server you are using is correctly set up, and still active.

  Use the External File Server test button to confirm the servers work.

2 Look in the Audit Trail portlet for the failed job.

3 Copy the "Executing read commands against the device" informational message content.

  For example:

  ```
  copy running-config tftp://192.168.0.138/010128030139_DefaultConfig
  ```

4 Use Direct Access to get to a Telnet / SSH command line on the device having backup issues.

  If you cannot get to a command line, then see Determining Incomplete Discovery on page 62 for the way to remedy that.

5 Paste the command you have copied in step 3 after the prompt.

6 Press [Enter].

7 Observe whether the device executes this command.

  If the device does not successfully execute the command, either the authentication used does not have permission to do such commands, or the device is configured to prohibit their execution.

  Consult with your network administrator to get the correct authentication, and either revise the Discovery Profile that discovered this device, delete the device from the OpenManage Network Manager system, and the discover it again. Or, Eeit the device and enter the revised authentication/management interface combination.

  If the device is configured to prohibit this command's execution, then consult the device's documentation and revise that.

8

Performance Monitoring

This section describes Resource Monitors as they appears in OpenManage Network Manager's web portal. The following describes these monitors:

- Application Server Statistics
- Resource Monitors
- Top N [Assets] (pre-configured monitor portlets that come with your installation by default.

Finally, this chapter contains a reminder about scheduling refreshes of monitor target groups. See Scheduling Refresh Monitor Targets on page 218.

If you see a monitor documented here that is unavailable in your installation, you may not have purchased it with your system's package. Consult your sales representative if you need to have the monitor that appears in documents, but not your installation.

NOTE:

If you configure your installation with multitenancy, you may be unable to edit Monitoring, except in the central, OpenManage Network Manager site. Collected statistics may be visible in the customer's domain as dashboards, but the configuration of the underlying monitor is not. Therefore, do not include a monitor portlet in the customer site template. Multitenancy does limit data dashboards and monitors display to the assets visible to the tenant sites as long as you create the dashboard on the tenant site.

Best Practices: Performance and Monitors

Monitoring can impact system performance. Monitors with many targets, many attributes per target and frequent polling intervals are most likely to slow system performance.

CAUTION:

Limit monitor targets to 10,000 or less per monitor (distribute them if you have more than 10,000). The following suggests other ways to improve monitor performance, too.

The following are the primary considerations when configuring monitors to get the desired performance from your system:

Database Insertion Rate — How many rows can your hardware realistically insert per second?

Every system has a maximum data insertion rate. This rate depends on the system's hardware configuration. A standard 7200 RPM disk can typically manage 300 insertions per second per disk. 10000-15000 RPM disk can have as many as 600 insertions per second per disk. Your experience may vary depending on your drive's controller and configuration.

The sum of all monitors' insertion rate should not exceed the system's maximum data insertion rate. To calculate the insertion rate of a monitor apply the following formula:

<# of monitor targets> x <# of retained attributes> / <polling interval in seconds> = inserts /second.

So a monitor with 100 targets, retaining 10 attributes once a minute would have an insertion rate of 17 rows per second (100 * 10 / 60 = 16.67 inserts per second).

Example:

Monitor A: 1000 targets * 10 retained attributes each / 120 = 83 insert per second

Monitor B: 100 targets * 25 retained attributes each / 600 = 4 insert per second

Monitor C: 10000 targets * 10 retained attributes each / 60 = 1667 insert per second

System total insertion rate (A+B+C): 1754 insertions per second

This configuration would be too aggressive for a system with a 7200 RPM disk since it dramatically exceeds the 300 insertions per second that the disk can support.

The following alternatives could resolve this:

- Upgrade to disk hardware that can keep up with the insertion rate. If the target insertion rate is 1754 inserts per second, add a disk to the array. If 1754 inserts / 300 insertions per second on a 7200 rpm disk amounts to 5.84 disks, use 6 disks (or more). If using 15000 RPM disks at 600 inserts per second, 1754/600 means you need 2.92 (3 discs) minimum.
- Modify the monitors to achieve a lower insertion rate. If you only have one 7200 RPM disk, it can only support 300 insertions per second. You have the option of lowering the target count, reducing what is retained or lengthening the polling interval.

So from the example above if we changed the polling interval from once a minute to once every 10 minutes, Monitor C's insertion rate would drop to 167 inserts per second. The overall system would then only have an insert rate of 254 per second well below the hardware's limitation.

NOTE:

Traffic flow analysis can process and retain even larger amounts of information. Flows that correlate 50%, polled every minute for a day require roughly 109G of database, and require 4500 insertions per second.

CAUTION:

These numbers and sample calculations represent best case scenarios. Any disk or disk array typically serves other applications and processes besides monitors. Make sure to take account of that when calculating how to accommodate your monitors. The system admin or system user should assist in making that assessment.

Storage Requirements (Database Size) — How much disk space do you need, based on your retention policy? See Retention Policies on page 174 for more about configuring those.

OpenManage Network Manager stores performance data in three different forms Detail, Hourly and Daily data. It collects Detail metrics directly from the device or calculates these from the collected data with each poll. Hourly data summarizes the detail data collected during the hour. Daily data summarizes the hourly data collected during that day. The retention policy associated to the monitor describes how long OpenManage Network Manager retains each of these data types within the system.

OpenManage Network Manager stores a performance metric as a single row within a database table. Each row in that database consumes roughly 150 bytes of disk space. The sum of each

monitor's disk space required determines the amount of disk space. For each monitor add the disk space required for the Detail, Hourly and Daily data using the following formula:

<Detail disk space> + <Hourly disk space> + <Daily disk space> = Monitor disk space in bytes

where...

<# of metrics retained per poll> = <# of monitor targets> x <# of retained attributes>.

<# of metrics retained per day> = <# of metrics retained per poll> x <# of polls per day>.

<Detail disk space> = <# of metrics retained per day> x <# of days to retain Detail data> x 150.

<Hourly disk space> = <# of metrics retained per poll> x <# of days to retain Hourly data> x 24 x 150.

<Daily disk space> = <# of metrics retained per poll> x <# of days to retain Hourly data> x 150.

If the system does not have sufficient disk space consider the following options:

- Add more hardware to increase the available disk space.
- Reduce the retention period of one or more monitors to lower the overall disk space requirements. Of the three data forms Detail data will consume the most disk space per day of retention.

Table size — Based on your monitor configuration how large will database tables get? Each monitor has a series of dedicated performance tables that store the Detail, Hourly and Daily performance metrics. The number of tables depends on the retention policy associated with the monitor.

A single table stores the monitor's detail data for a 24 hour period. Detail data are individual performance metrics collected and/or calculated during each poll. After that initial 24 hours, OpenManage Network Manager creates a new table to store the next 24 hours' of detail data and so on.

Because of the resulting table size, the number of performance metrics generated by a single monitor in a 24 hour period impacts performance. Best practice is to configure each monitor to produce less than 10 million rows per day. When monitors exceed that number noticeable delays result when retrieving performance data. To determine the number of metrics retained by monitors per day please refer to <# of metrics retained per day> calculation from the previous section.

△ CAUTION:
These numbers depend entirely upon the system hardware, available memory and processor speed.

If a monitor does exceed the target maximum rows per day consider the following options singly or in combination to change that:

- Reduce the number of retained attributes per poll.
- Reduce the polling frequency.
- Reduce the number of monitor targets per monitor. Notice that you can still have the same number of targets if you split the targets among multiple monitors.

Finally, tune your database for the expected load. Refer to the *OpenManage Network Manager Installation Guide* for MySQL sizing recommendations.

Dashboard Performance Limits

Creating dashboards makes performance demands on your system. If you make too many, or monitor too many attributes within your dashboards, system response times can suffer. Performance can also suffer because you have too many dashboard portlets on a single page.

To work around these limitations, add another page (see Portal Overview on page 442 for details), then move some dashboard portlets from the over-populated page to the new one. You can also split monitored attributes between different dashboards.

Monitoring from a Cloud Server

The following outlines hardware sizing for performance monitoring from a cloud server

RAM	Maximum Targets (polling: 5 minutes intervals)	Heap Memory Settings	Recommended CPU cores and Disk Space
16 GB RAM	10000	4 GB Synergy Web Server heap, 6 GB Application Server heap, 2GB Database buffer	4+ core, 100 GB+ disk space
32 GB RAM	25000	6 GB Synergy Web Server heap, 12 GB Application Server heap, 8 GB Database buffer	4+ core, 200 GB+ disk space
64 GB RAM	50000	8 GB Synergy Web Server heap, 16 GB Application Server heap, 24 GB Database buffer	8+ core, 400 GB+ disk space
128 GB RAM (recommended)	50000	12 GB Synergy Web Server heap, 24 GB Application Server heap, 48 GB Database buffer	16+ core, 400 GB+ disk space

Caveats

- VPN tunnel is assumed to be available to cloud services
- The suggested target number are for latency under 50ms. You may have to scale down numbers of targets when latency is greater than 50ms.

monitorTargetDown Event Interval

By default, OpenManage Network Manager only creates the monitorTargetDown event every 30 minutes, even if the polling interval is shorter. This behavior is configurable. There are properties through which you can either tell the system to always create these so-called availability events every time it finds the target unreachable.

You can also change the time threshold for which it will create another monitorTargetDown event if you want to have these created more or less often then once every 30 minutes in circumstances where a polling target remains unreachable for an extended period of time.

To configure this interval, modify (or better, override) the following properties (from `.../owareapps/performance/lib/pm.properties`)

```
#Monitor alarm settings
#
#pm.monitor.AlwaysReemitAlarm=true
#pm.monitor.AlarmReemitTimeout=15
```

Notice that these are commented out by default, so monitorTargetDown appears by 30 minute intervals, and the default for `AlwaysReemitAlarm` is `false`. Restart application server for edits to take effect. In a cluster, all edits must be consistent.



How To:
Configure Monitors

This chapter contains the following step-by-step instructions for these features:

- Create a Server Status Monitor Dashboard
- Create an SNMP Interface Monitor
- Create an ICMP Monitor
- Create a Key Metrics Monitor
- Create an Adaptive CLI Monitor
- Create a Monitor for an External Script
- Create a Monitor Report
- Create a Simple Dashboard View
- Create A Performance Template

You can see Performance Options from a variety of locations by right-clicking in OpenManage Network Manager. For example:

- Ports in the Ports portlet
- Interfaces
- Ports / Interfaces in the Details panels lets you *Show Performance*
- Right clicking on any of the above within a Reference tree lets you select Performance Options.
- All Top N [Assets] portlets let you right click for Performance options.

Monitoring Strings

Monitors do not directly monitor string attributes, but you can create an extractive Adaptive CLI monitor that responds to string values in devices. See Example 5: Monitor Text Values on page 303 for an example.

Monitor Life Cycle

The following diagrams illustrate OpenManage Network Manager's performance monitoring process.

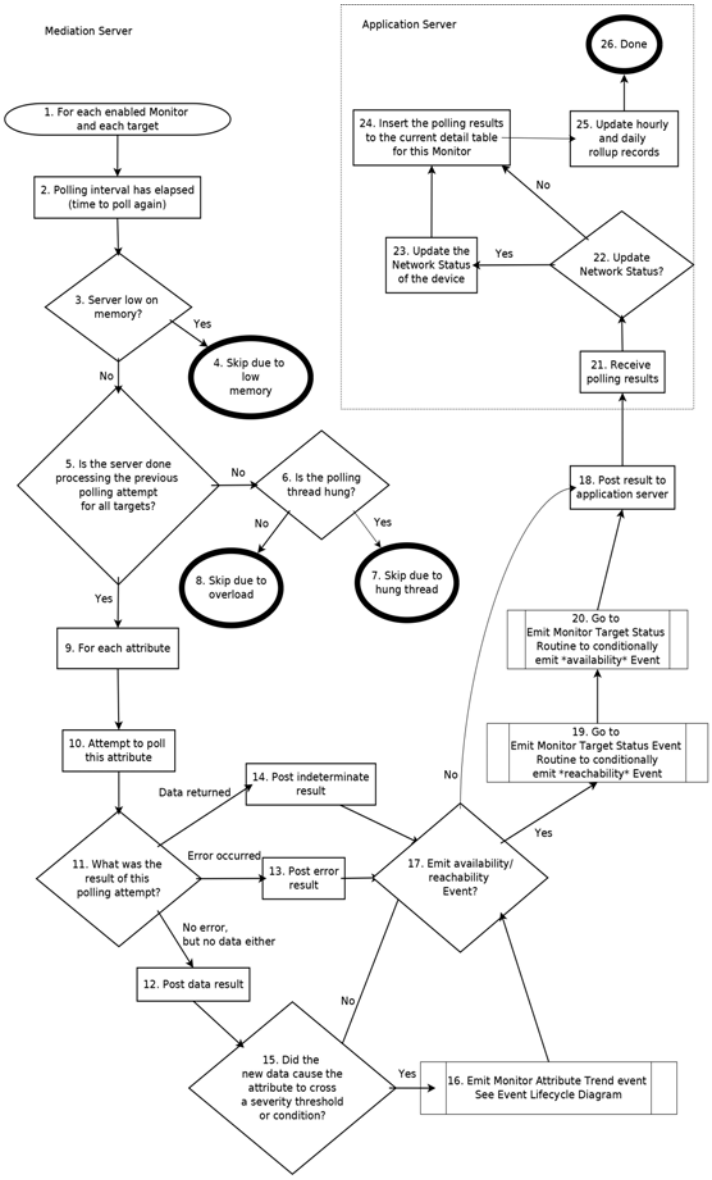
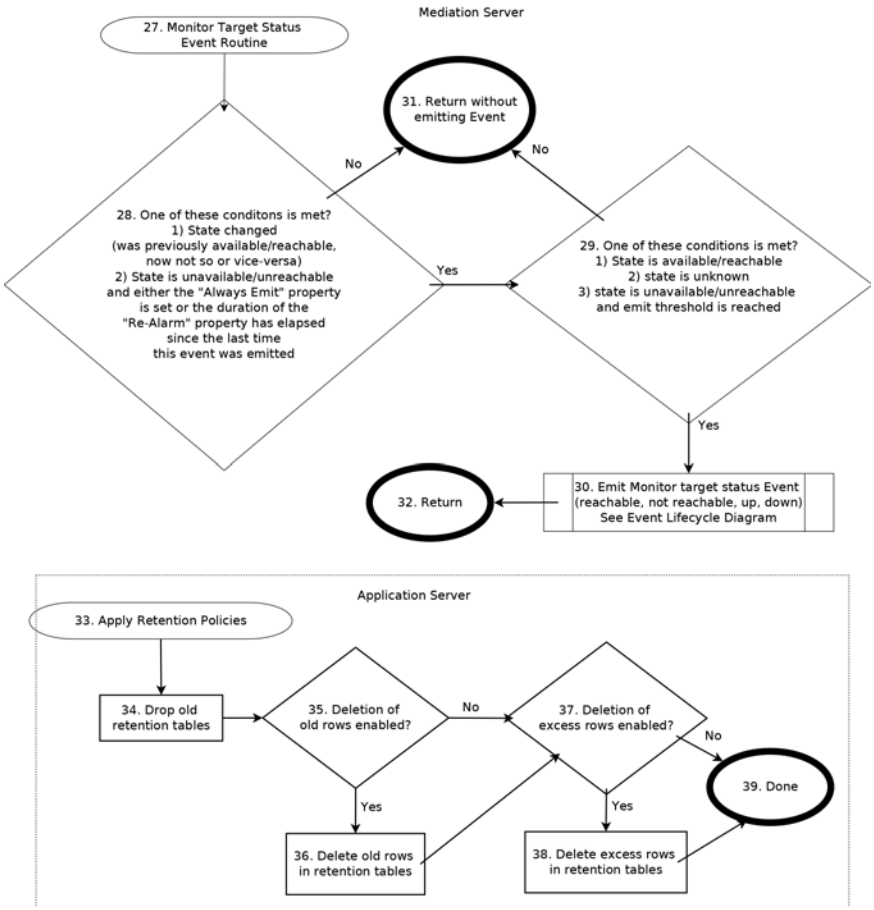


Diagram 2:



Performance Monitor Life cycle Legend

1. **For each enabled Monitor and each target**—This process executes for each item within the Resource Monitors portlet that is marked as Enabled and for each targeted entity.
2. **Polling interval has elapsed**—This process executes every time the Polling Interval has elapsed. For example if the Polling Interval for a given Monitor is 15 Minutes then it executes that often.
3. **Server low on memory**—Is the server low on memory? This is determined by the property `lower.threshold.limit` which by default is 5. This means that if the available memory on the server is less than 5% (or whatever value this property is set to) then it meets this condition.
4. **Skip due to low memory**—Numbers 4, 7 and 8 all involve skipping rather than trying to poll the targeted entity. If OpenManage Network Manager finds the system low on memory then it cannot poll the target(s) and skips polling instead. Any time it skips it increments the associated skip count and also updates the associated last time skipped. You can view these attributes can be viewed through the *JMX console* > *oware* > *service=PollingEngine*. See `SkippedExecutionDueToMemoryCount` and `MostRecentSkippedExecutionDueToMemory`.

5 **Is the server done processing the previous polling attempt for all targets?**—Is the server still working on polling targets from the previous time? The polling process begins every time the polling interval elapses, regardless of whether or not the server is still working on the previous round of polling.

   This means the previous polling attempt has not produced results so the server will have to skip it (due to overload) rather than trying to perform two (or more) polling attempts simultaneously. If the polling interval is short enough then there will inevitably be skips due to overload because the polling process takes time.

6 **Is the polling thread hung?**—Is the polling thread hung? If so it is not doing any work and will not produce any results. There is a maximum duration that a polling thread has to produce results before the polling engine considers a thread hung. The PollingEngine MBean attribute `ThreadInterruptThreshold` which is set to 90000 (15 minutes) by default determines this.

7 **Skip due to hung thread**—Similar to number 4. If a polling thread is hung then it cannot poll the target(s) and will instead skip. Any time it skips it will increment the associated skip count and also update the associated last time skipped. View these attributes through the JMX console > oware > service=PollingEngine. See `HungThreadInterruptedCount` and `MostRecentHungThreadInterrupted`. When the system identifies a hung polling thread it tries to interrupt the thread and reclaim it.

8 **Skip due to overload**—Like number 4. If the server is overloaded then it cannot poll the target(s) and will instead skip. Any time it skips it will increment the associated skip count and also update the associated last time skipped. View these attributes through the JMX console > oware > service=PollingEngine. See `SkippedExecutionDueToOverloadCount` and `MostRecentSkippedExecutionDueToOverload`.

9 **For each attribute**—Every Monitor has a set of attributes that it will try to periodically poll from each targeted entities.

10 **Attempt to poll this attribute**—OpenManage Network Manager tries to reach the target device and poll the given attributes.

11 **What was the result of this polling attempt?**—Was this target available and reachable? If so did data return for this attribute? Certain error conditions result from an error occurring, including if the connection failed or was refused or dropped or if there were bad credentials or if there was a device fault. Some conditions result in posting an indeterminate result, including the data context not being found within the device for the attribute being polled.

12 **Post data result**—OpenManage Network Manager posts attribute data it successfully retrieves from the target device. Once it posts this data to the application server and stores it in the database, because data returned, the Monitor Status Summary of the target device becomes *Available* (with a green checkbox icon) in most cases.

   The only exception occurs when not all requested attributes for the target returned data. If some data returns but one or more attributes is unavailable or not supported by the device then status of the target says *Partial Results* (with a yellow triangle with an exclamation point icon).

   Note that this step compiles the polling data that came from the target device, it does not post the returned data to the application server nor store it to the database, but it does identify the polling results as successful, as opposed to error or indeterminate.

13 **Post error result**—If an error occurred during the attempt to poll the target then OpenManage Network Manager posts information about the error. Possible causes: connection to the target failed, was refused, or was dropped, bad credentials, or another device fault. Once

OpenManage Network Manager posts the error information to the application server and stores it in the database, the Monitor Status Summary of the target device becomes *Not Available* (with a red "X" icon). Note that this step exists only to take note of the errors that occurred during the last polling attempt. Like step 12, this step does not post any data to the application server nor store it to the database, but simply compiles the results of the last polling attempt.

14 **Post indeterminate result**—Sometimes the attempt to poll the target device is indeterminate. In such situations, neither an error occurred, nor did any data return from the target. If OpenManage Network Manager did not find the data context on the target device for this attribute, or a timeout occurred while trying to reach the device, this can occur. Once OpenManage Network Manager posts the indeterminate information to the application server and stores it in the database, the Monitor Status Summary of the target device becomes *Not Applicable* (with a gray question mark icon). Like step 12, this step does not post any data to the application server nor store it to the database, but simply compiles the results of the last polling attempt.

15 **Did the attribute to cross a severity threshold or condition because of the new data?**—Each attribute can have one or more severity thresholds and/or conditions. For example if the CPU usage exceeds 95% then its attribute might be at a critical severity level. If an attribute was previously within a certain severity level and the new polling results show that this attribute crossed the threshold into another severity level (for example minor to major or major to critical) then it meets this condition. If new polling results show that this attribute remained in the same severity level (for example, it was critical and remains critical at least for the moment), then it does not meet this condition.

16 **Emit Monitor Attribute Trend Event**—OpenManage Network Manager emits a monitorAttributeTrend Event. Go to step *1. RC internal trap occurred* of the Understanding Event Life Cycle diagram.

17 **Emit availability/reachability Event**—An *Emit Availability* checkbox appears on the *Editing Monitor* popup screen. When you check it, OpenManage Network Manager creates reachability Events.

18 **Post result to application server**—In distributed environments, much of this processing is going on within the mediation server. Once OpenManage Network Manager produces the polling results, it adds them to a queue that the server then reads. In effect, OpenManage Network Manager has posted the results to the application server. Once the application server receives these results, it inserts them into the database for later querying. Monitor this queue through the JMX console > oware > service=MonitorPollingHandlerMBean.

19 **Go to Emit Monitor Target Status Event Routine to conditionally emit reachability Event**—Go to step 27, the Emit Monitor Target Status Event Routine, to consider the *reachability* of the target device. This routine computes whether to emit the reachability Event.

20 **Go to Emit Monitor Target Status Event Routine to conditionally emit availability Event**—Go to step 27, the Emit Monitor Target Status Event Routine, to consider the *availability* of the target device. This routine computes whether to emit the availability Event.

21 **Receive polling results**—Here, the application server receives polling results from the mediation server.

22 **Update network status?**—The Update Network Status checkbox on the *Editing Monitor* popup screen determines whether this condition is met.

23 **Update the network status of the device**—OpenManage Network Manager updates the network status of the device based on the polling results that were created in steps 12, 13 or 14.

24 **Insert the polling results to the current detail table for this Monitor**—OpenManage Network Manager inserts the polling results into the detail table associated with this Monitor so that they can be queried later.

25 **Update hourly and daily rollup records** —OpenManage Network Manager updates the hourly and daily rollup records for this attribute.

26 **Done**—Processing on the application server is done until more polling results are received from the mediation server.

27 **Monitor Target Status Event Routine**—This routine is executed to compute whether or not to emit the Monitor target status Event, which will either be for the reachabilityEvent or the availabilityEvent. There are similar conditions that determine whether these types of Events are emitted.

28 **Is one of these conditions met? State change, always emit, re-emit timeout**—Are any of these conditions met?

- The state changed with the last polling attempt. Either the device was previously available/reachable and now it is notavailable or notreachable or vice versa. If the state is the same as before (for example, it was unavailable and this is still the case) then it does not meet this condition.

- The state is unavailable/unreachable and one of the follow two sub-conditions is met:

a. The `pm.monitor.AlwaysReemitAlarm` property is set to true. This property is set to false by default.

b. The duration of the `pm.monitor.AlarmReemitTimeout` property has elapsed since the last time OpenManage Network Manager emitted a Monitor target state Event for this particular target and Monitor. By default this property is 30, which means that by default even if a polling target stays down for a period of several hours, it will only emit this Event at most every 30 minutes. Even if you configure the Monitor to poll this target more often than this and even if this target is unavailable every polling cycle, it will still only emit this Event every 30 minutes, unless you change this property.

29 **One of these conditions is met?**—Available, unknown, or threshold reached? (State is unavailable/unreachable and threshold for the number of unreachable/unavailable attempts has been reached).

This threshold comes from the *# of Unreachable Attempts before update* field on the *Editing Monitor*. Note that this field covers both unreachable and unavailable attempts.

30 **Emit Monitor target status Event**—Emit the Monitor target status Event. If this routine was called to consider the reachability of the target then it will emit one of these two types of Events: monitorTargetReachable and monitorTargetUnreachable. Similarly if this routine was called to consider the availability of the target then the Event that is emitted will either be of the type monitorTargetUp or monitorTargetDown (in this context "Up" and "Down" is shorthand for available and not available). Go to # 1. RC internal trap occurred of the Event Life cycle diagram.

31 **Return without emitting Event**—Return the origin of this routine without emitting an Event.

32 **Return**—Return to the origin calling this routine.

33 **Apply Retention Policies**—This begins the process that applies retention policies to drop tables and/or delete rows from tables.

34 **Drop old retention tables**—Drop the retention tables that are old according to the retention policy for the monitor associated with each table.

35 **Deletion of old rows enabled?**—Most often, the only way old polling data is aged out of the system is by dropping the old tables but there is also a property that controls whether or not to delete old records within the tables without dropping the tables completely. This property is `pm.retention.DeleteOldDBRecords` and is false by default. This feature was added in an earlier version of OpenManage Network Manager to deal with limitations that existed in older database versions that are no longer supported. We strongly recommend keeping this feature disabled because it is produces a significant drag on system performance and does not provide any added benefit beyond the dropping of expired tables (and all the data within them), which occurs anyway.

36 **Delete old rows in retention tables**—OpenManage Network Manager deletes the old rows in the retention tables according to the retention policy for the monitor associated with each table.

37 **Deletion of excess rows enabled?**—A property controls whether to delete excess records within the retention tables without dropping the tables completely. This property is `pm.retention.PruneRowsInRawDataTablesToMaxCount` and it is false by default. If you set this property to true, then the value of the property `pm.retention.RawDataMaxCount` is the maximum number of rows that any retention table can have. This feature existed in earlier versions of OpenManage Network Manager to deal with limitations that existed in older database versions that are no longer supported. We strongly recommend keeping this feature disabled because it is a significant drag on system performance.

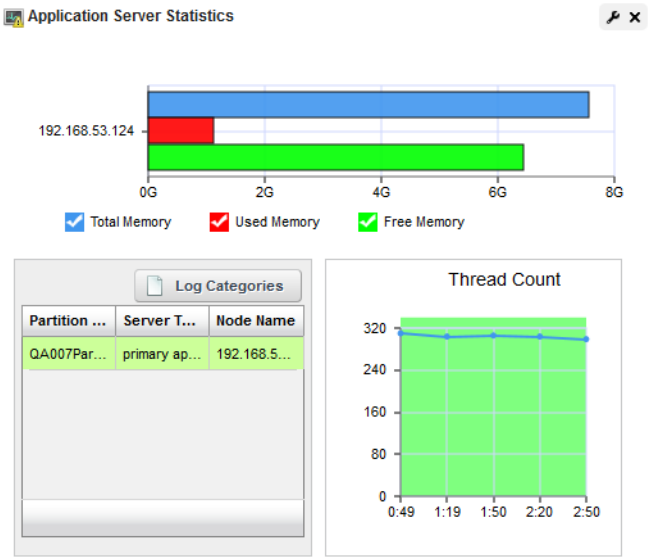
38 **Delete excess rows in retention tables** —OpenManage Network Manager deletes the oldest rows in the retention tables to get the row count down to the maximum accepted number.

39 **Done**—Done applying retention policies for polling data.

Application Server Statistics

The Application Server Statistics portlet has no expanded view. It displays the statistics for the OpenManage Network Manager application servers and provides access to set logging levels for a variety of categories on application servers.

By default, this portlet is available from the Settings page by selecting the Server Configuration menu option.

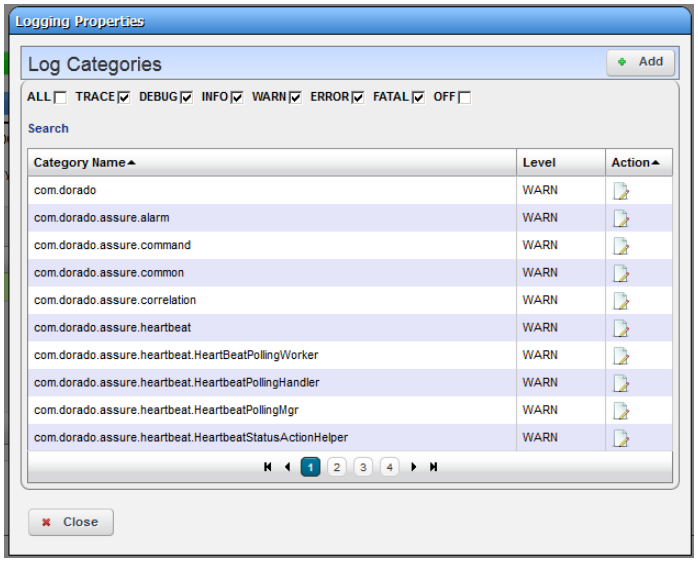


The bar graph displays *Total*, *Used*, and *Free* memory on the server. One such graph appears per server monitored. Hover your cursor over a bar to see its reading in a tooltip. Hover your cursor over the bar graphs related to the server you want to monitor, and its information appears in a tooltip.

The Thread Count graph displays information for as long as this portlet is open, restarting when you revisit it or refresh the page.

Logging Categories

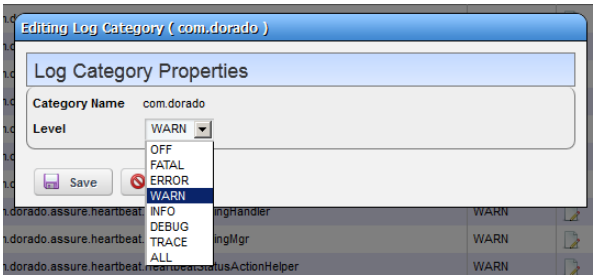
The Application Server Statistics portlet also displays a table that catalogs servers' *Partition Name*, *Server Type* and *Node Name*. This includes a button the upper right corner where you can access *Log Categories*—`log4j.xml` items—without having to text edit that file. See *Defining a Custom Debug* on page 82 for more about `log4j.xml`.



The `log4j.xml` items appear listed with their default log levels. Altering log levels for the listed items can provide more information for troubleshooting. Log levels determine the detail of server log output.

Notice that you can sort these by clicking the table headings, and can look for items with the *Search* link below the checkboxes. You can check or uncheck categories at the top of this screen to confine the display to only desired categories.

These self-monitoring capabilities let you tune Application Server logs to produce meaningful output. Clicking the Edit icon to the right of an item lets you change its log level.



NOTICE

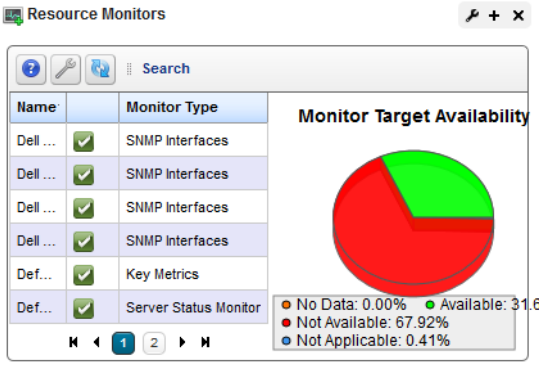
Changing log levels in this screen alters log reporting levels for all Application servers, if you have more than one, without restarting them. This simplifies setting log levels, and does not require editing the log4j.xml file.

CAUTION:

More, and more detailed logging can have a performance impact. See also Best Practices: Performance and Monitors on page 157.

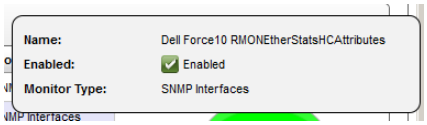
Resource Monitors

This summary screen displays currently, active performance monitors in brief.



The *Name* column displays the identifier for each monitor instance, *Enable* displays a green check if it is currently enabled, or a red minus if it is disabled.

The *Monitor Type* column typically displays what the monitor covers. Hover your cursor over this



column to see a popup with the selected monitor's properties. The popup that appears after this query displays the relevant information for the monitor, including whether it is *Name*, *Enabled*, and *Monitor Type*.

The graph that appears to the right of the monitors displays the aggregate availability information for the enabled monitors. Topics graphed include, *Available*, *Not Available*, *No Data* and *Not Applicable*.

Yellow icons mean that not all the data requested was collected. This can occur when MIB attributes have been deprecated. Typically, OpenManage Network Manager monitors include alternative attributes.

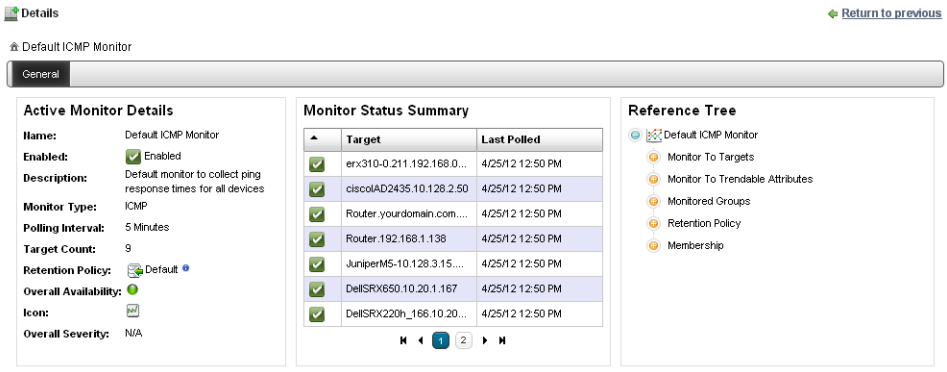
Right-click a listed monitor to do the following (not all menu items appear for all types of monitors):

New Monitor—Lets you either create a new monitor of the type you select in the sub-menu, or edits the monitor selected in the portlet. See Monitor Editor on page 176 for details.

New (from Template)—Opens the Monitor Editor, where you can configure the equipment targets for preconfigured monitor templates of the type(s) selected in the sub-menu. These templates are based on monitors described in Monitor Options Type-Specific Panels on page 196, but have already have selected attributes and calculations. You can examine exactly what these are in the editor that appears when you select one.

Edit Monitor—Opens the Monitor Editor, where you can modify the selected monitor. For a look at the individual monitors' screens, see Monitor Options Type-Specific Panels on page 196.

Details—Opens a Detail panel, with a reference tree, status summary, and general information about the selected monitor.



Copy Monitor—Copy the selected monitor and its settings to make a new monitor. You must re-name the copy, and can change settings selectively.

Enable / Disable Monitor—Enables or disables the monitor. Only one of these options appears. Only enabled monitors report data (and demand resources), while disabled monitors do not.

Refresh Monitor— Re-query to update any targets for the current monitor. See Scheduling Refresh Monitor Targets on page 218 for instructions about automating this.

Manage Retention Policies—Select this to manage the data retention policies for the selected monitor. See Retention Policies on page 174 for details.

Delete—Removes the selected monitor.

View Monitor Data—View the targets' responsiveness to the monitor. Red means unresponsive, green means responsive, and yellow means intermittently responsive.

View as PDF—Creates an Acrobat PDF document containing this alarm's contents displayed in the summary portlet.

Import/Export—Export the selected config file to disk, or import it from disk. You can also import/export a selected configuration file.

Provides the following actions when available for the selected image:

- Import retrieves a file containing XML compliance descriptions. Some imports can come from a URL.
- Export Selection exports the selected description to an XML file.
- Export All exports all descriptions to an XML file.

Click Download Export File to specify where to save the file.

The Import/Export option is useful as a backup or to share descriptors with other projects.

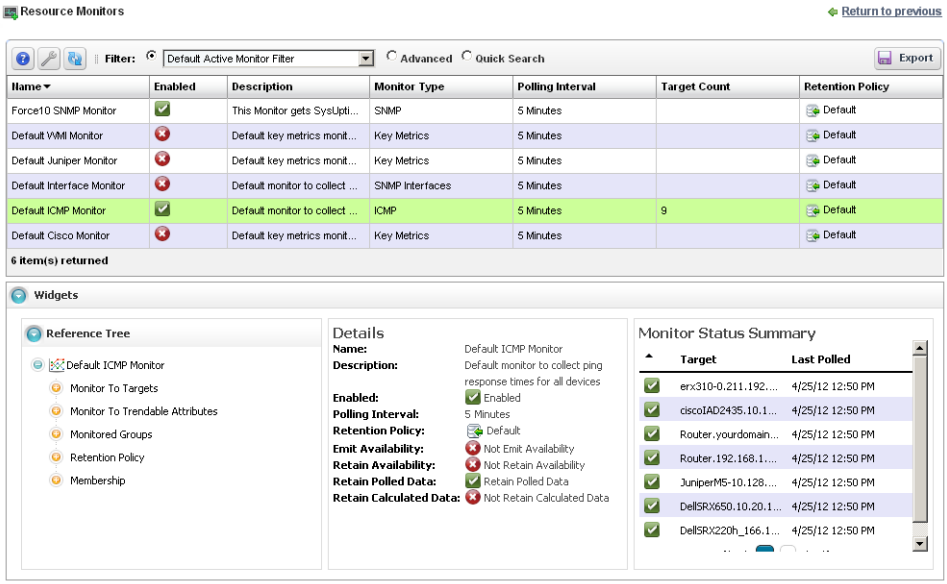
You must import data into the correct portlet. For example, you cannot import event data into the Actions portlet.

If one type of data depends on another, you must import the other data before importing the data that depends on it.

Share with User—Opens the Share with User window where you select the colleague you want to share this assets with and then type your message.

Expanded Resource Monitor

This screen appears when you click the plus in the upper right corner of the summary screen.



As in most expanded views, this one displays a list ordered by the *Name* of the monitor. Click *Settings* to configure the column display. Available columns include those on the summary screen (*Name*, *Enabled*, *Monitor Type*) as well as *Description*, *Poling Interval*, *Target Count* and *Retention Policy*. Menu items are like those described for the summary portlet.

Resource Monitor Snap Panels

When you select a monitor, the Snap Panels at the bottom of the screen display details about it. The *Reference Tree* shows the selected monitor's connection to attributes, groups, retention policies and its membership (the devices monitored).

The *Details* Snap Panel displays the attributes the popup shows when you hover the cursor over the *Monitor Type* column in the summary screen, and adds *Emit Availability* (events), *Retain Availability*, *Retain Polled Data*, and *Retain Calculated Data* parameters.

The *Monitor Status Summary* Snap Panel displays the status of each individual member (*Target*) of



the monitor, showing the *Last Polled* time and date, and a title bar and icon indicating *Availability* (green is available, red is not).

Hover the cursor over the Availability icon, and a popup appears with details about availability. If the device is available, the *RTT* (round-trip time) for communication appears in *Avg* (average), *Max* (maximum), and *Min* (minimum) amounts, along with the *PacketCount*. If it is not, an *Error Message* appears instead of the *RTT* and *PacketCount* parameters.

To edit more performance settings and targets than are available here, use the features described in Dashboard Views on page 223. You can create and display dashboards by right-clicking items in the Managed Resources portlet, selecting *Show Performance*.

Excluding Attributes from Display

The `show.perf.exclude` property in the `portal-ext.properties` file contains a comma delimited list of the attribute display names to exclude from display. Remember, best practice is to override properties as described in Overriding Properties on page 71.

For example,

```
show.perf.exclude=CPU Utilization,AvgRTT
```

If you define this property, the *Show Performance* command creates charts for the listed attributes. This has no impact on manually created dashboards.

NOTE:

You must restart tomcat after changing the properties file for the changes to take effect.

How To:

Monitor Network Availability— Alternative Method

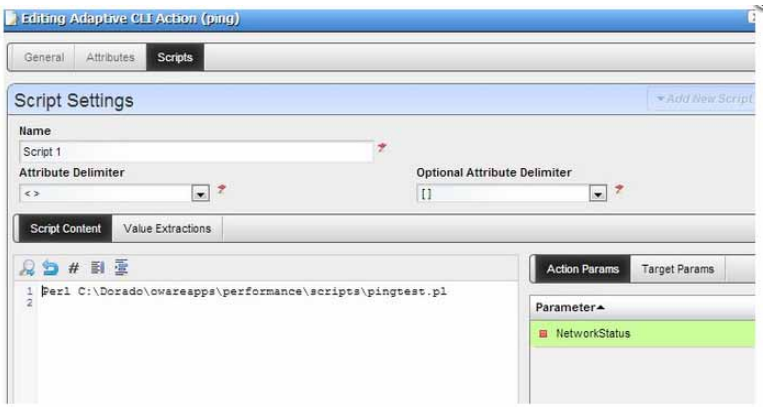
In addition to using the standard ICMP monitor, you can create performance monitors that return network availability information displayed on monitor tooltips and reflected in the Network Status column in the Managed Resources portlet.

Here are the steps to set that up:

1 Create an Adaptive CLI that monitors some status attribute. For example, rather than using the built-in ICMP ping on OpenManage Network Manager, you can use a Perl script like this one:

```
use Net::Ping;
$hostname = '10.128.7.11';          # host to check
$timeout = 10;                # how long to wait for a response
print "-1" if pingecho($hostname, $timeout);
```

2 Make sure the script's network-monitoring attribute return maps to an Adaptive CLI integer attribute named or containing *NetworkStatus*. (NetworkStatus can be just part of the attribute name. It is case insensitive.) You must add this attribute to the Adaptive CLI.



3 Configure the data extraction as follows:

Attribute Name: NetworkStatus

Parse Algorithm: Extract

Parse Expression: (/-*/d)$

4 Create an Adaptive CLI monitor referring to your Ping script Adaptive CLI.

5 Configure it to monitor the attribute in the selected Adaptive CLI as follows:

Attribute Name: Network Status (or your name containing that)

Attribute Type: Integer

Enabled: [check]

Metric Type: Gauge

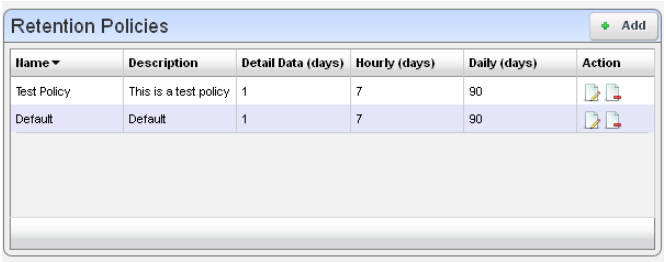
Also make sure to check the *Update Network Status* checkbox on the monitor.

6 If this attribute exists and the value is 1, polling sets the device's network availability to *Available*. If its value is 0 it sets availability to *Not Available* and if it is -1 it sets availability to *Indeterminate*.

Retention Policies

The basis of all reporting and dashboard presentations is data retained from monitors. In other words, each monitor provides a simple schema from which you can produce a chart, graph or report.

All monitors rely on a polling engine which executes device interactions at regular intervals. To



reduce resource impacts, you can exclude some of the collected data from what OpenManage Network Manager retains. A monitor could even have no retained data, only emitting events based on transient results in the execution/calculation. Another example: the application can derive a metric from several collected values and you may opt to retain only the derived result. Monitors may share a retention policy.

OpenManage Network Manager rolls up data hourly and daily into aggregations. See the Aggregate Data on page 175 for more details. The retention policy controls how long OpenManage Network Manager holds data per aggregation period. You must select the correct period if you want to review what has been collected.

When you select *Manage Retention Policies* in the Monitors portlet, first a list of available policies appears. Clicking the *Add* button at the top of the screen lets you create a new policy, while clicking the *Edit* button to the right of selected, listed policies lets you modify existing policies. The *Delete* button to the right of listed policies removes them from the list.

Editor

Monitors may share a retention policy. The retention policy controls how long data is held per roll-up period. The editor for Retention policies lets you assign characteristics and monitors to them.



The editor contains the following fields:

General Retention Policy Options

Policy Name—A text identifier for the policy.

Description—An optional description for the policy.

Detail / Hourly / Daily Data (Days)—How many days to retain the selected data.

The amount retained has both a performance and data storage impact. For example, retaining day's information from an active performance SNMP monitor configured with one target's worth of data, retrieved on one minute intervals can consume 0.7 G of database, and require 21 insertions per second. See Best Practices: Performance and Monitors on page 157 for more about retention policies, monitors and how they impact performance.

Active Monitor Members

Select from *Available Monitors* on the left, and click arrows to move the desired monitor(s) to the *Selected Monitors* on the right.

Click *Save* to preserve your edits, and include the monitor as listed among existing Retention Policies, or click *Cancel* to abandon any changes.

Aggregate Data

OpenManage Network Manager uses detail polling data to produce aggregate values for larger intervals of time, including hourly and daily periods. Here is how this works: at the end of each hour, the detail polling data for the previous hour is aggregated (or as we can say "rolled up") into hourly data. The resulting hourly records are always given the polled time that is the start of the hour, but these data points represent the aggregation across the entire hour. For example, if there is a monitor that polls its targets every 5 minutes, then during the 10 am hour it will poll 12 times and it will have results for each target and for each attribute for each time it polls. Then when the 11 am hour begins, OpenManage Network Manager will aggregate all of the detail polling data collected between 10:00 am and 10:59 am and these new hourly data points will be given the polled

time 10:00 am. Likewise, at the end of each day, OpenManage Network Manager will aggregate all hourly data into daily data, and all new daily data points will be given the polled time of midnight of the previous data. These daily data points should be understood to represent an aggregation across the entire day.

You can also report on longer aggregation periods, including Weekly, Monthly, Quarterly, and Yearly, but these values are computed on-the-fly and are not stored in the database. See Create a Monitor Report for more information about how to generate reports for monitoring data.

Deployment and Polling of Monitor Targets

For each active monitor, the polling targets are deployed and OpenManage Network Manager polls the appropriate attributes every interval. There are two ways of defining the targets for a given monitor: explicit and implicit. Explicit targets are defined by selecting the specific devices that should be polled (equipment managers, subcomponents, etc.) Implicit targets are defined by configuring a monitor to poll a group of devices, where the group implicitly includes certain devices based on certain filter criteria. Explicit targets can only be added or removed if you edit the monitor. Implicit targets can be added and removed any time a device is added or removed from inventory or some attribute of a device changes. When implicit targets are removed from a monitor, they are not deleted but they are changed from active to inactive. Only active targets are deployed. Inactive targets are not deployed, but you can still report on the polling data that is associated with inactive targets.

Also, for each monitor target, the Equipment Manager that the target is associated with has a Device Management State, and this data is copied over into an attribute of the monitor target itself. Only targets whose Device Management State is Normal will be deployed. For example, if a monitor target is an interface of a device in inventory whose Management State is Decommissioned, then this target will not be deployed. As long as the Management State is something other than Normal, this target will never be deployed and OpenManage Network Manager will never poll the device, even if the target is active. See Create a Monitor Target Report on page 195 for more information.

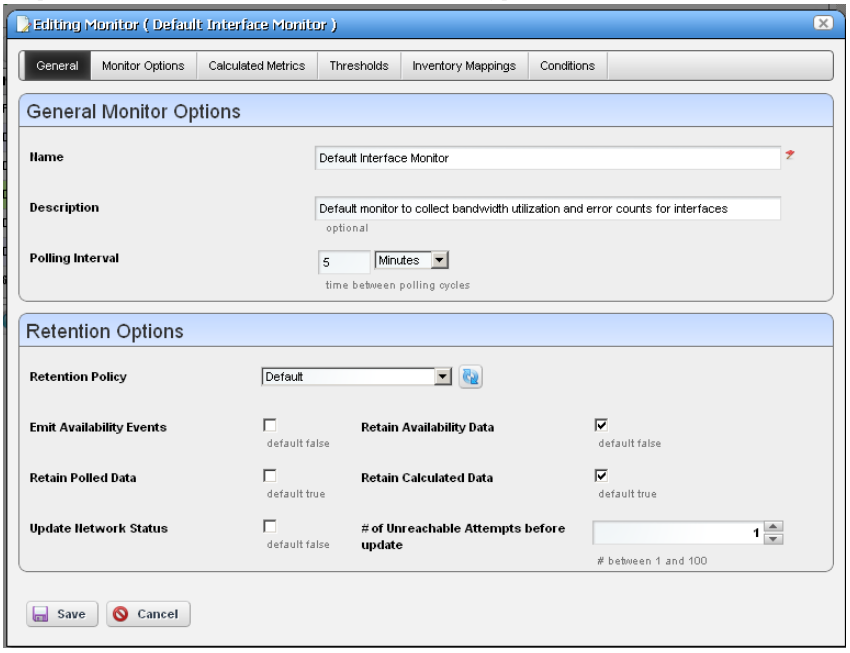
Monitor Editor

This editor lets you fine-tune the monitor you selected and right-clicked to open the editor. It includes the following panels and fields:

- General
- Monitor Options
- Calculated Metrics
- Thresholds
- Inventory Mappings
- Conditions

General

The General panel is common to all different monitor types.



General Monitor Options

Name—The identifier for this monitor.

Description—A text description for this monitor.

Polling Interval—Use these fields to configure how often the monitor polls its target(s).

Retention Options

Retention Policy—This configures how long OpenManage Network Manager retains the monitor's data. Manage these by right-clicking in the Resource Monitors portal, and selecting *Retention Policies*. You must make retention policies before you can select them here. See also Retention Policies on page 174.

Enabled—Check to enable.

Emit Availability Events—Check to activate emitting availability events. The monitor does not emit an event until the monitored entity's state has changed. All monitors can generate events on failure to contact the monitored device, port, and so on. For example, by default ICMP monitor updates the network status after a selected number of consecutive failures.

You can configure the monitor to generate an event in addition to updating network status, but OpenManage Network Manager does not like the polling interval to be very small especially when monitoring many devices.

Example: poll every 10 secs for 10,000 devices with Packet Size = 64 bytes, Packet Count = 3 Timeout (secs) = 1, and configure Unreachable attempts = 1 with polling interval = 10 seconds. This polls the device every 10 seconds and emits a "down" event on the first failed attempt.

Retain Availability Data—Check to activate. You must Retain availability data to enable alarms. If you define thresholds, you should retain availability data. *Retain availability data* stores the Boolean values of whether availability data was in the range your defined metrics.

Retain Polled Data—Check to activate. If you uncheck *Retain polled data* only calculated data remains, you cannot view data retrieved from monitored entities. Turning off *Retain polled data* discards the data as it arrives from the device.

Retain Calculated Data—Check to activate. *Retain calculated data* complements *Retain polled data*. If checked, it stores the calculated results which came from the raw poll data received from the device.

Update Network Status—Check to activate reporting the network status of the target device(s). The results of this monitor's activity then appear in the Network Status column of the Managed Resources portlet. Only one monitor—and no monitors on interfaces or child components—should ever update networks status. Any monitors on child components or interfaces are rolled up to the top level device, so status may be erroneously reported. For example the top level device is not necessarily down if the interlace is down.

If two monitors report the network status of a single device on different intervals, they must both agree it is down before that state appears in Managed Resources. As long as one monitor says a device is *Responding*, then that is the state displayed.

If ping fails (an endpoint is down) and update network status is configured, then OpenManage Network Manager tries to ping the switch/router in front of the endpoint to determine if that device is reachable. If that device also failed, then the endpoint's status becomes *indeterminate*.

NOTICE

For clarity's sake, best practice has only one monitor per device updating network status. By default ICMP monitoring enables *Update Network Status*, and monitors all discovered devices.

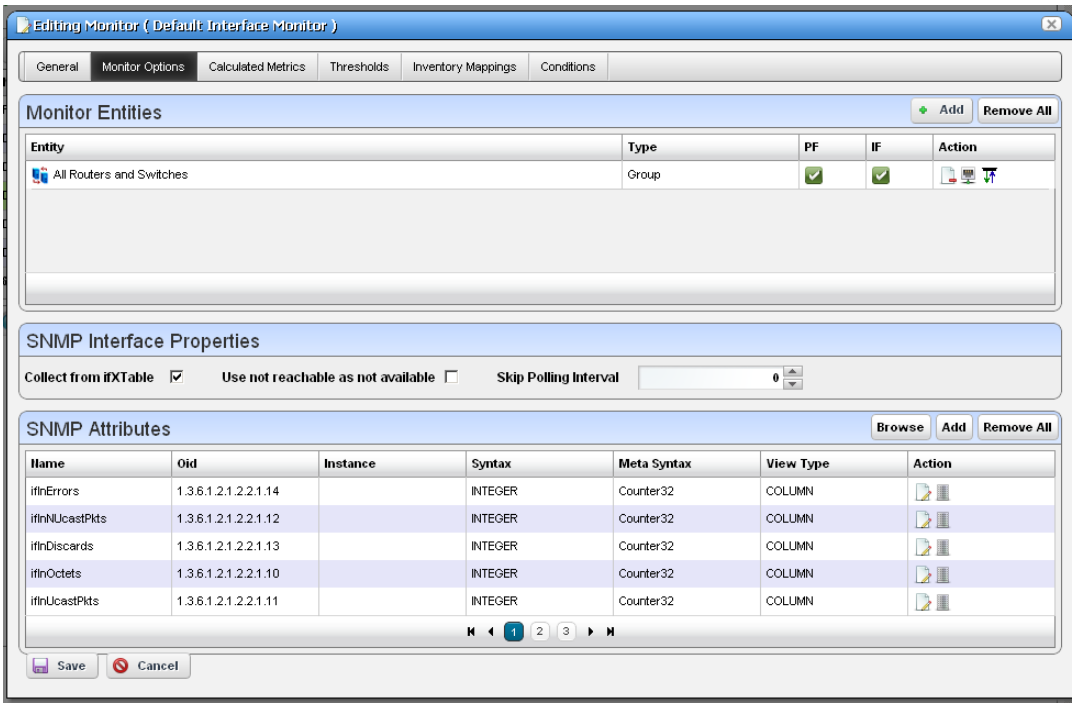
Migrating from previous OpenManage Network Manager versions automatically replaces any configured Heartbeats with ICMP monitors with *Update Network Status* enabled. If your previous system had HTTP or SNMP heartbeats, you must manually configure monitors to provide equivalent monitoring in this version.

# of Unreachable Attempts before update—The number of attempts to reach the device before OpenManage Network Manager updates the displayed network status of the device. (1-100)

Click *Save* to preserve any edits you make, or *Cancel* to abandon them.

Monitor Options

Monitor options contains two panels. The entity panel lets you select the monitor targets. The types of monitor entities allowed varies depending on the type of monitor. The second panel contains options specific to the monitor type being edited.



The entity and options panels for the various types of monitors appear below in Monitor Options Type-Specific Panels on page 196.

CAUTION:

Have no more than 20,000 targets on a single monitor. Your system may not keep up with polling if you exceed the recommended target limit. Best practice is to poll important devices in shorter intervals and less important devices over longer intervals.

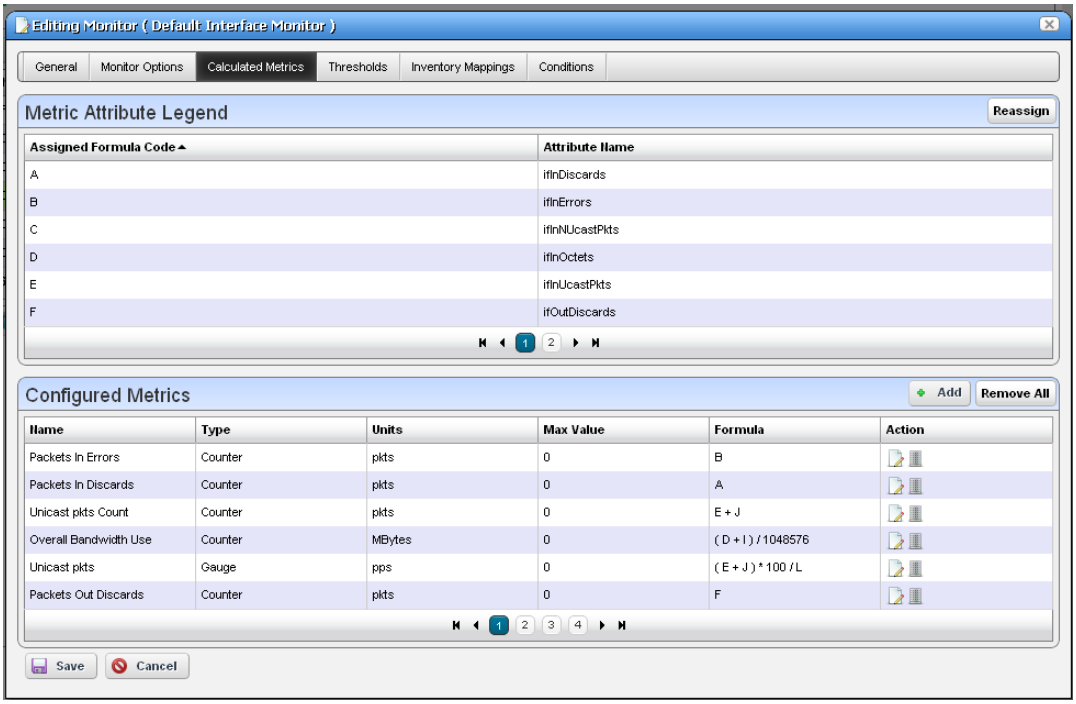
NOTICE

You can elect to monitor the same attribute in multiple, different monitors. This has a performance impact. Best practice is to monitor an attribute only once.

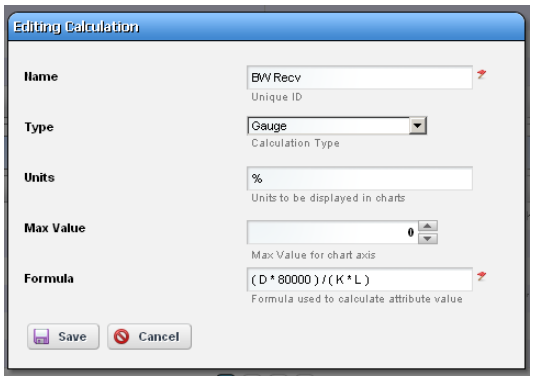
Calculated Metrics

The calculated metrics panel lets you create attributes that are calculated from existing monitor attributes. The metric attribute legend assigns a letter value to each monitor attribute. The *Reassign* button reassigns the letters. This is useful if some attributes have been deleted and their letters are no longer used.

The *Configured Metrics* table lists the calculated metrics. An edit and delete action appears to the right of each row. The *Add* button creates a new calculated metric and the *Remove All* button deletes all the calculated metrics.



Clicking on the Add button or edit button displays the calculation editor.



This panel contains the following properties:

Name—The attribute name to be displayed for the calculation

Type—Calculation Type - Gauge or Counter

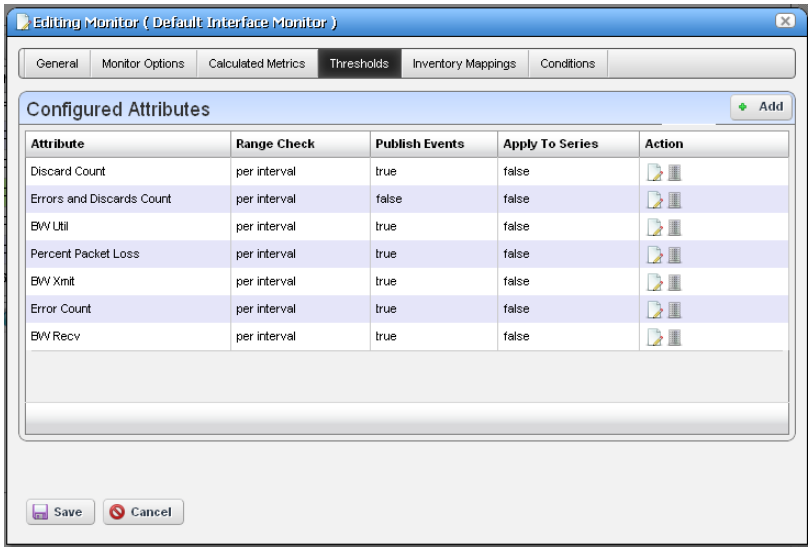
Units—Units string to appear in graphs. Units do not appear in dashboards with a single attribute.

Max Value—Maximum value to be used in graphing (0 = no max)

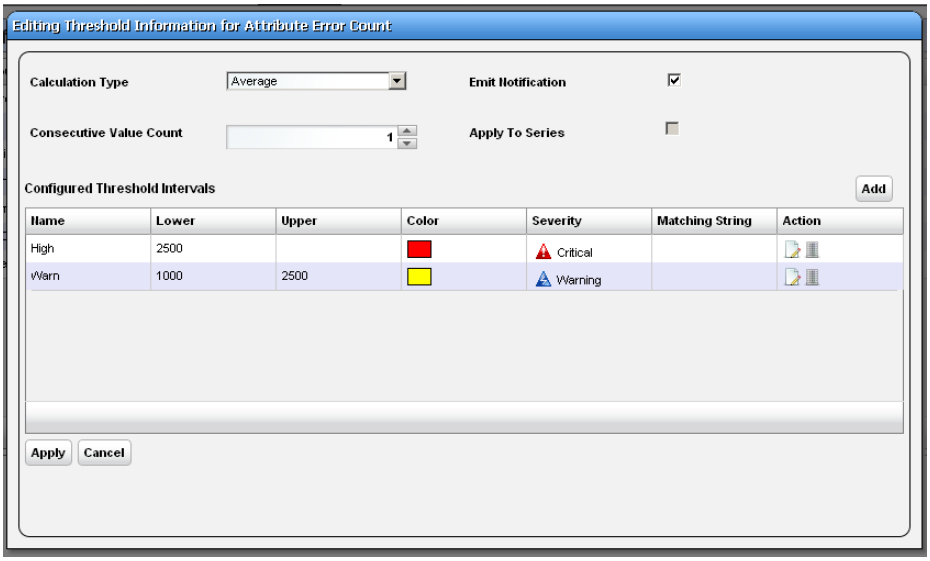
Formula—The formula for the calculation using the assigned formula codes from the metric attribute legend.

Thresholds

The thresholds panel allows the user to set threshold intervals on attributes in the monitor. The table lists the attributes for which attributes have been configured. Each row has an edit action and delete action. The Add button allows thresholds to be specified for another attribute. If all monitor attributes have thresholds defined for them the Add button will be disabled.



The *Add* or *Edit* buttons open a threshold editor (blank or with existing, configured thresholds, respectively).



Configure threshold intervals you *Add* at in the editor screen according to the following parameters.

Attribute Name—Appears when you click *Add* rather than *Edit*ing a selected threshold. Use the pick list that appears in this screen to select the attribute for which you are specifying threshold information. When you *Edit*, the name of the attribute appears as a title within the editor screen.

Calculation Type—Select from the pick list. Specifies whether the range calculation is to be done based on *Average* or *Consecutive* values.

Consecutive Value Count—Select how many consecutive values to consider at once for a range calculation. Typically the larger the number here, the less "flutter" in reporting threshold crossings.

Emit Notification—Check to emit an event if the device crosses the configured threshold(s). The notification event contains the threshold-crossing value, as well as which threshold was crossed, and is an alarm at the severity selected when you configure the threshold.

You can make a set of thresholds for each monitored attribute, so a single monitor can throw different alarms for different attributes. To see available events and their descriptions, view the contents of the RedcellMonitor-MIB in `\owareapps\performance\mibs`.

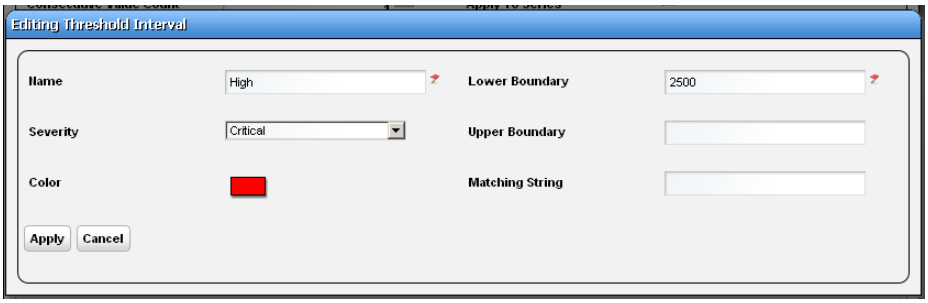
Apply to Series—Check to enable on composite attributes only. Checking this applies the threshold to individual elements within the series. When it is unchecked, the threshold applies only to aggregate measurements (the overall value of the series), not individual elements within the series.

For example; a Key Metric monitor for CPU utilization on a device with two CPUs actually monitors both CPUs. When unchecked, the threshold applies to the average of both CPUs, when checked, the threshold applies to each individual CPU.

You can also apply thresholds to regular expressions. This is useful to monitor components within components, for example cores within a CPU.

Click *Apply* to preserve your edits, or *Cancel* to abandon them.

The threshold interval editor pops up when you select the *Add* button or the *Edit* icon to the right of a threshold's row in the threshold attribute editor.



This screen contains the following fields:

Name—The identifier for the threshold interval.

Severity—The event severity for crossing this threshold interval (*informational/indeterminate/warning/minor/major/critical*)

Color—The color to display threshold interval on graphs.

Lower Boundary—The interval's lower boundary.

Upper Boundary—The interval's upper boundary. May be blank.

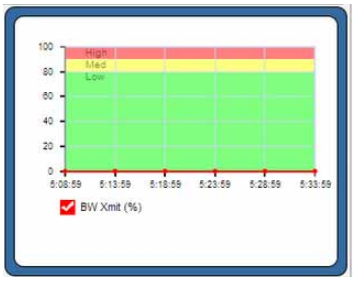
Matching String—A Regex matching string.

NOTICE

You can configure a response to threshold crossing with an Event Processing Rule. Create your thresholds within the monitor and then create an Event Processing Rule whose filter conditions respond to `monitorAttributeTrend` and other conditions such as severity, and so on. You can even use specific values of the event varbinds in the filter conditions too.

Threshold Graph Background

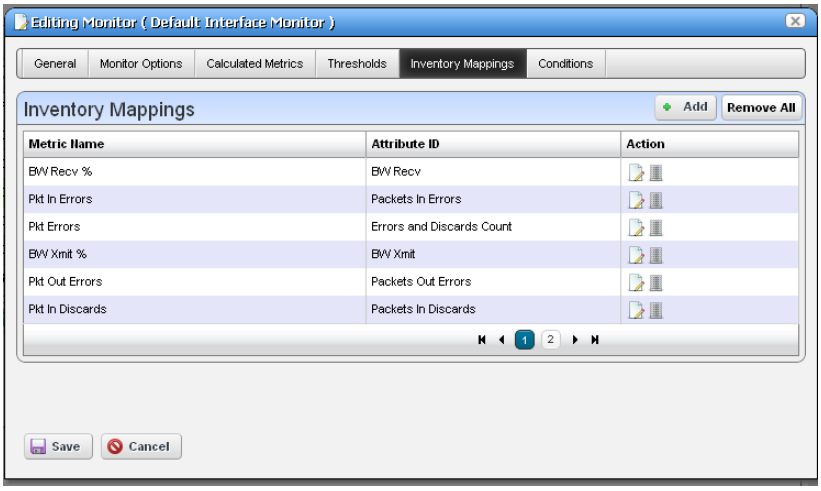
If you configure a set of thresholds, the dashboard graph displaying the data monitored displays the



threshold colors (and text label) in the background. When an upper or lower threshold has no upper or lower bound, then those background colors may appear as white.

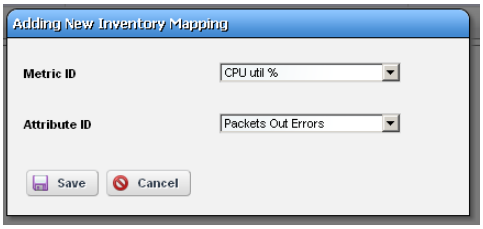
Inventory Mappings

The inventory mappings panel lets you associate predefined inventory metrics with a monitored attribute to normalize the attribute if a device does not report metrics in a way that matches the monitored attribute's name or format. Available metrics include *CPU Utilization %*, *Memory Utilization %*, *ICMP Round Trip Time*, *ICMP packet errors*, and *Bandwidth utilization %*.



Common attributes include those for Top N. For example, service A may call it "Disk % Utility" and Service B may call it "% Disk Utility". We can map them to a common name and can display them as Top N.

You can *Add* a new mapping with that button, or *Remove All* listed mappings with that button. You can also edit or delete listed mappings with the *Action* icons to the right of each row. Adding or editing opens the Inventory Mapping Editor.



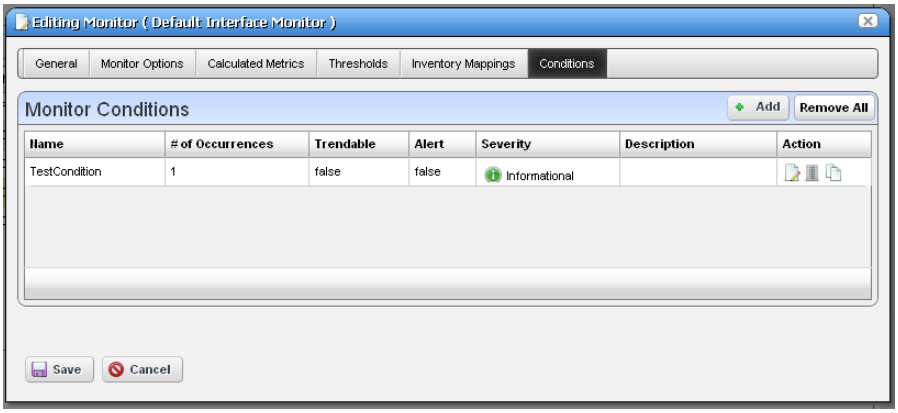
This lets you configure the following:

Metric ID—Inventory metric name

Attribute ID— Attribute to associate with the inventory metric

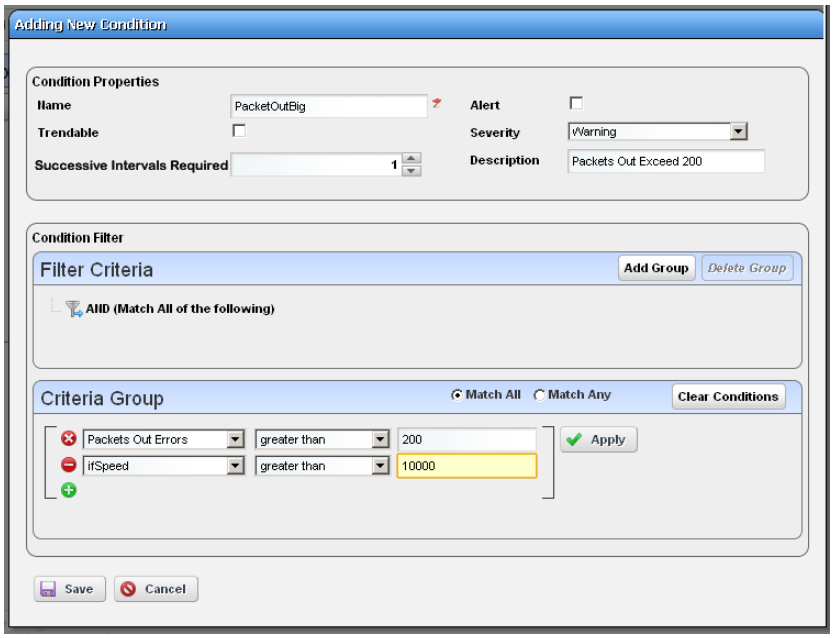
Conditions

This panel lets you add multiple conditions to the monitor you are editing.



Click the *Add* button to enter a new set of conditions, or click the *Edit this entry* button to the right of a listed Monitor Condition to open the editor. Click the *Delete* button to remove a listed set of conditions. Click the *Copy* icon to duplicate the listed condition.

The editor has the following fields and settings to configure:



Condition Properties

Name— Enter a text identifier for the conditions.

Alert— Check this if you want OpenManage Network Manager to emit an alert when the monitor satisfies the conditions.

Trendable— Check if the conditions specified are trendable. If this is true, the database retains qualifying conditions (or thresholds) for later reporting / dashboards.

Severity— Specify the severity of the emitted alert, if any.

Successive Intervals Required— Enter the number of occurrences of what is specified in the Condition Filter to satisfy the Conditions.

Description— A text description for the conditions.

Condition Filter

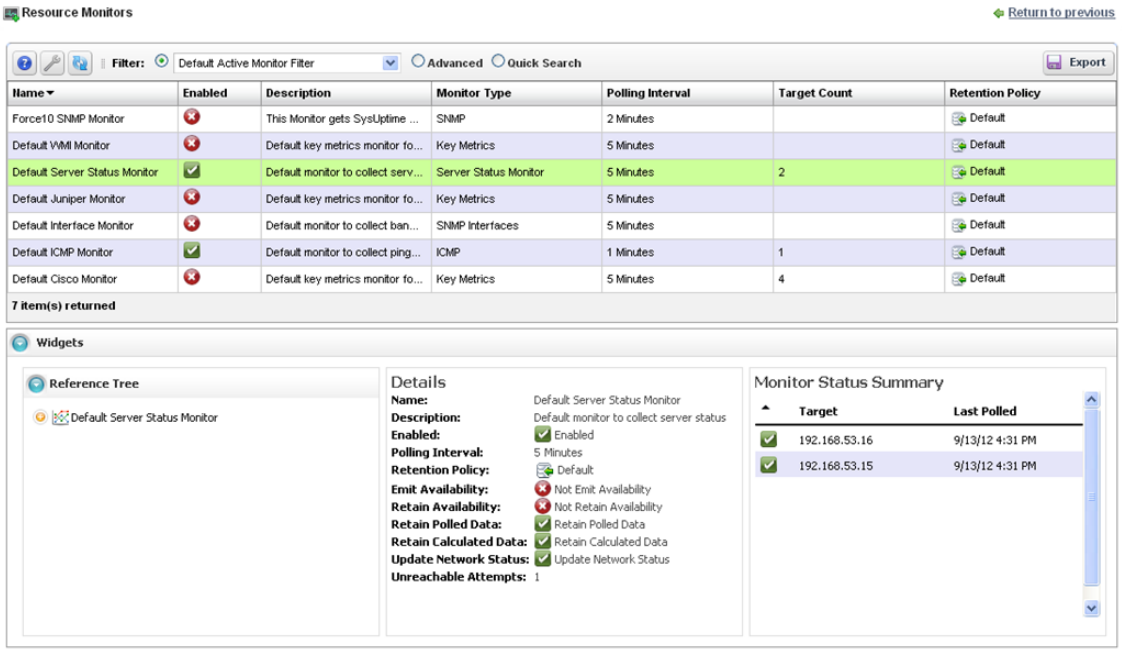
Minimally, use this panel to select a condition, an operator and a value. If you want to use the logical AND or OR operators with a second condition, click the green plus (+), and select a second condition, operator and value. For example, *Packet Out Errors greater than* 200 AND *ifSpeed greater than 10000* can be a set of conditions that only has to occur once to satisfy this monitor's condition.

Click *Save* to accept your edits, or *Cancel* to abandon them.

Self Management / Self Monitoring: Default Server Status Monitor

OpenManage Network Manager also includes a Default Server Status Monitor that monitors its own server(s). Even clustered application and mediation servers are automatically added to this monitor. You can edit this monitor to alter polling intervals, and make different calculations for the

monitored attributes. Those attributes include TotalMemory, FreeMemory, MemoryInUse, ThreadCount and TrapCount for Application Server and Mediation Server processes. You cannot modify the targets for this monitor.



You must create your own Dashboard to view the data in this monitor. Create a custom dashboard for this as in described below.

How To:

Create a Server Status Monitor Dashboard

1. Create a custom dashboard as described in How to: Create a Custom Dashboard View on page 228.
2. Click the edit icon on one of the dashboard components and set the data source as the Default Server Status Monitor, and the target as the server(s) monitored.
3. Save the monitor

See Dashboard Views on page 223 for more about configuring dashboards.

How To:

Create an SNMP Interface Monitor

To set up a typical performance monitor, follow these steps:

1. In the *Resource Monitors* portlet, and create a new monitor by right-clicking and selecting *New*.

2 Select the type of monitor from the submenu—for this example, an *SNMP Interfaces* monitor.

NOTE:

Some devices have ports rather than interfaces. This monitor works for them too, even though it is an "interface" monitor.

3 In the *General* screen, enter a polling interval (5 minutes is the default). For this example, check *Retain polled data* and accept the remaining defaults for checkboxes and the retention policy.

4 Select an entity to monitor by clicking the *Add* button in the top portion of the *Monitor Options* screen. For an interface monitor, select *Interface* as the Type at the top of the screen. You can also filter the list of interfaces that appear further by selecting *Interface Type* as *ge* (gigabit ethernet), for example.

NOTICE

Notice that you can add refinements like filtering on *Administrative State* and *IP Address* to the filter.

5 Select interfaces (Ctrl+click to add more than one), then click *Add Selection* then *Done* to confirm your entity. Hover your cursor over a line describing an interface to have a more complete description appear as a popup.

6 Click *Browse* to display the MIB Browser. For the sake of this example, we elect to monitor ifInErrors (in RFC Standard MIBs, RFC1213-MIB > Nodes > mib-2 > interfaces > ifTable > ifEntry > ifInErrors).

7 In the *Thresholds* screen, configure thresholds by first clicking *Add*.

8 Click *Add* above the threshold levels list for each threshold you want to add.

9 In the threshold editor, enter a name (Examples: *Low*, *Medium*, *Overload*), an upper and lower boundary, (0 - 10, 10 - 100, 100+), a severity (*Informational*, *Warning*, *Critical*) and color (BLUE, YELLOW, RED). In this case, no string matching is necessary. When the data crosses thresholds, the monitor reacts.

Attributes available depend on the type of monitor you are creating. Notice that you can also check to make crossing this threshold emit a notification (an alarm that would appear on the Alarm panel). You can also configure the type of calculation, and so on. You can even alter existing thresholds by selecting one then clicking *Edit* to the right of the selected threshold.

10 Click *Apply* for each threshold interval you configure, then *Apply* for the entire threshold configuration.

If a threshold's counter is an SNMP Counter32 (a 32-bit counter) monitoring can exceed its capacity with a fully utilized gigabit interface in a relatively short period of time. The defaults configured in this monitor account for this, but if you know that this is an issue, you can probably configure the monitor to account for it too.

After taking a look at Thresholds no more configuration is required. Notice, however, that you can also configure *Calculated Metrics*, *Inventory Mappings* and *Conditions* on other screens in this editor to calculate additional values based on the monitored attributes, to map them, and to make conditional properties based on monitored behavior.

NOTICE

Calculated Metrics is particularly valuable if you want to monitor a composite like ifInErrors + ifOutErrors or want to calculate a parameter like errors per minute when the monitor's interval is 5 minutes.

11 Click *Save* and the monitor is now active.

Notice that the *Availability* icon appears at the top of a *Monitor Status Summary* snap panel in the Expanded Resource Monitor next to a time/date stamp of its last polling. Right-click the monitor and select *Refresh Monitor* to manually initiate polling.

Values displayed in the Overall Availability column of the Monitor Manager do not automatically refresh and may be out of date. The *Reference Tree* snap panel maps the monitor's relationship to its target(s) attribute(s) and other elements. The *Details* snap panel summarizes the monitor's configuration.

12 For information about having the monitor's results appear in the a *Dashboard* portlet, see *Dashboard Views* on page 223.



How To:
Create an ICMP Monitor

The following steps create an ICMP (ping) monitor.

1 In the *Resource Monitors* portlet, and create a new monitor by right-clicking and selecting *New*.

2 Select the type of monitor from the submenu—for this example, an *ICMP* monitor.

3 In the *General* screen, enter a name (Test ICMP Monitor), and a polling interval (5 minutes is the default). For this example, check *Retain polled data* and accept the remaining defaults for checkboxes and the retention policy.

4 Select an entity to monitor by clicking the *Add* button in the top portion of the *Monitor Options* screen.

5 Select devices you want to ping, (Ctrl+click to add more than one), then click *Add Selection* then *Done* to confirm your entity.

6 Define packets in the ICMP Monitor Options panel, including Packet Size, Packet Count and timeout. You can accept the defaults here, too.

7 In the Thresholds tab, select an attribute (MaxRTT, or maximum round trip time) and add the following thresholds by clicking *Add*:

Name *High* color red, Lower Boundary 15 and Upper Boundary [blank] Severity *Critical*

Name *Fine* color green, Lower Boundary 0 and Upper Boundary 15 Severity *Cleared*.

Notice that this example does not emit a notification. If you checked that checkbox, an alarm of the configured severity would accompany crossing the threshold.

8 Accept the other defaults and click *Apply*

9 Click *Save*.

10 Test ICMP Monitor now appears in the portlet.



How To:
Create a Key Metrics Monitor

Follow these steps to create a Key Metrics Monitor (also, see Key Metric Editor on page 236).

1 In the *Resource Monitors* portlet, and create a new monitor by right-clicking and selecting *New*.

2 Select the type of monitor from the submenu—for this example, an *Key Metrics* monitor.

3 In the *General* screen, enter a name (Test Key Metrics Monitor), and a polling interval (5 minutes is the default). For this example, check *Retain polled data* and accept the remaining defaults for checkboxes and the retention policy.

4 Select an entity to monitor by clicking the *Add* button in the top portion of the *Monitor Options* screen.

5 Select devices on which you want to monitor Key Metrics.

6 Select from the available metrics that appear at the bottom of the screen in Key Metric Properties by selecting a category with the pick list at the top of the screen, then click on an *Available* metric, and click the right arrow to make it a *Selected* metric.

7 Click *Save* to retain your new Monitor.

8 Test Key Metrics Monitor appears in the Resource Monitors portlet.



How To:

Create an Adaptive CLI Monitor

You can create monitors that track Adaptive CLI responses. The following outlines the steps:

1 Determine the Show Command that you want to run.

2 Create ACLI to extract the data as described below.

3 Create the Monitor that uses the data from the ACLI.

4 Create any threshold crossing events/actions (see Thresholds on page 181).

5 Create dashboards (see Dashboard Views on page 223) to view results and reports (see How to: Create a Monitor Report) to preserve or display the data.

Monitor Reports in Multitenant Environments

Reports for the master site can target all available devices, however, in tenant sites, only devices to which the tenant site has access are visible in reports.

If, for example, a tenant wants to make a report about a monitor shared by all tenants, then the tenant can create the report only for data from devices assigned to its site.

Show Command

For this example, use the Cisco `show ip traffic` command. Run the command so you can see the data you want to extract. Here, we want to know the number of dropped packets due to adjacency and no route issues. Here is some example output:

```
c1720-1.30#show ip traffic
IP statistics:
  Rcvd:  2072045 total, 1995503 local destination
         0 format errors, 0 checksum errors, 0 bad hop count
         0 unknown protocol, 0 not a gateway
         0 security failures, 0 bad options, 0 with options
  Opts:  0 end, 0 nop, 0 basic security, 0 loose source route
         0 timestamp, 0 extended security, 0 record route
         0 stream ID, 0 strict source route, 0 alert, 0 cipso, 0 ump
         0 other
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
         0 fragmented, 0 couldn't fragment
```

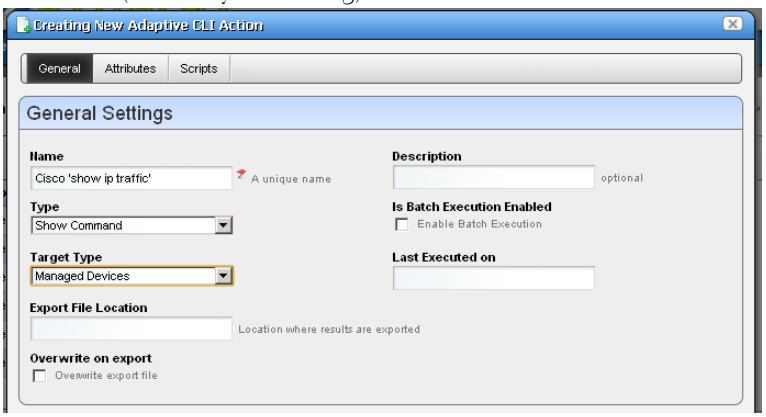
```
Bcast: 1952255 received, 4 sent
Mcast: 0 received, 0 sent
Sent:  86915 generated, 0 forwarded
Drop:  18 encapsulation failed, 0 unresolved, 0 no adjacency
       0 no route, 0 unicast RPF, 0 forced drop
```

This command has more output, our only concern is extracting the number of no routes and no adjacencies in the first section, underlined, above.

Create ACLI

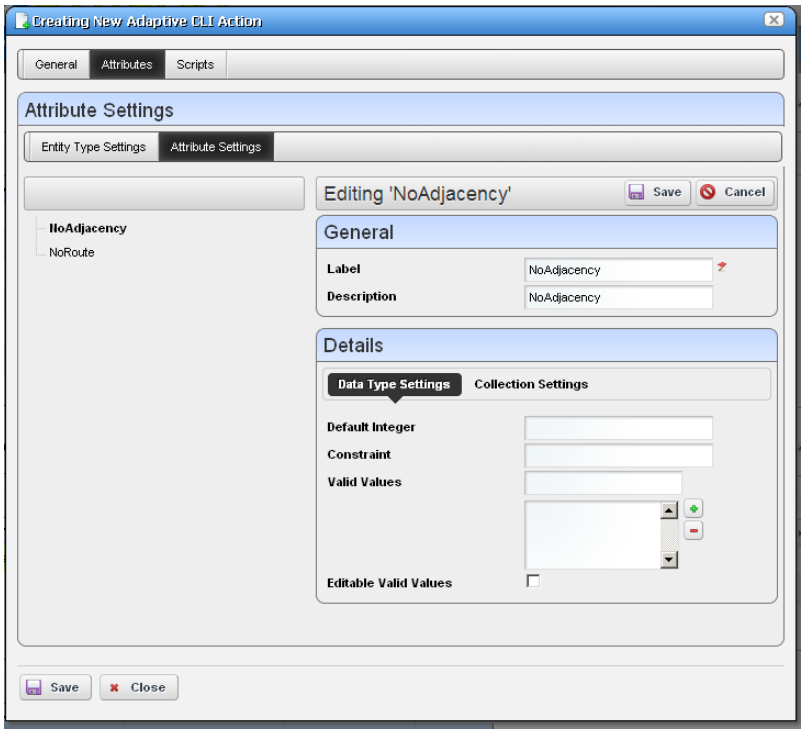
Create a *show* ACLI for the `show ip traffic` command. This ACLI executes the command and it will extract the appropriate data using RegEx.

1 Create a new ACLI (or modify an existing)



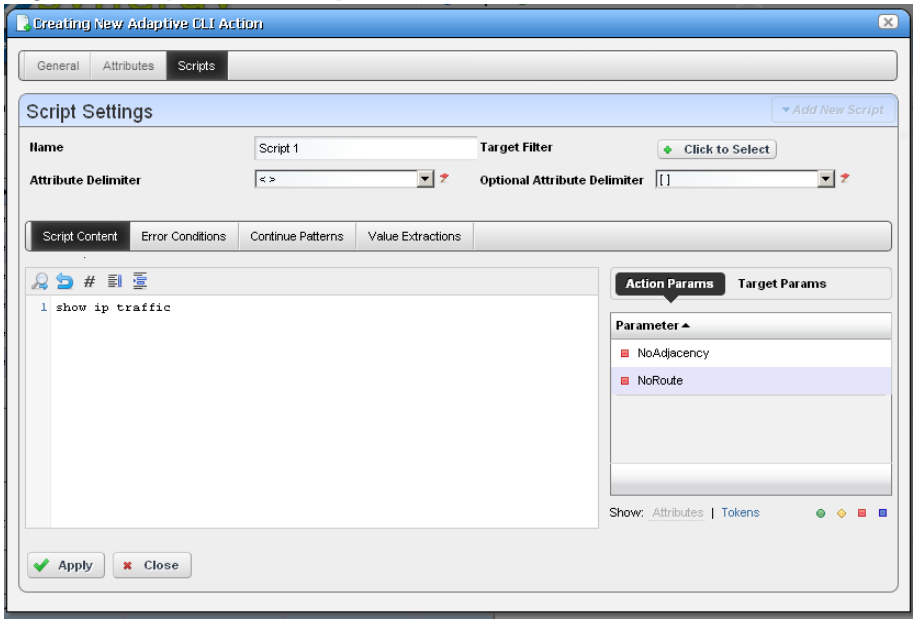
Create an attribute in ACLI for each attribute that you want to monitor. The Date Type must be Integer.

2 Here, there is an attribute for `no_adjacency`.



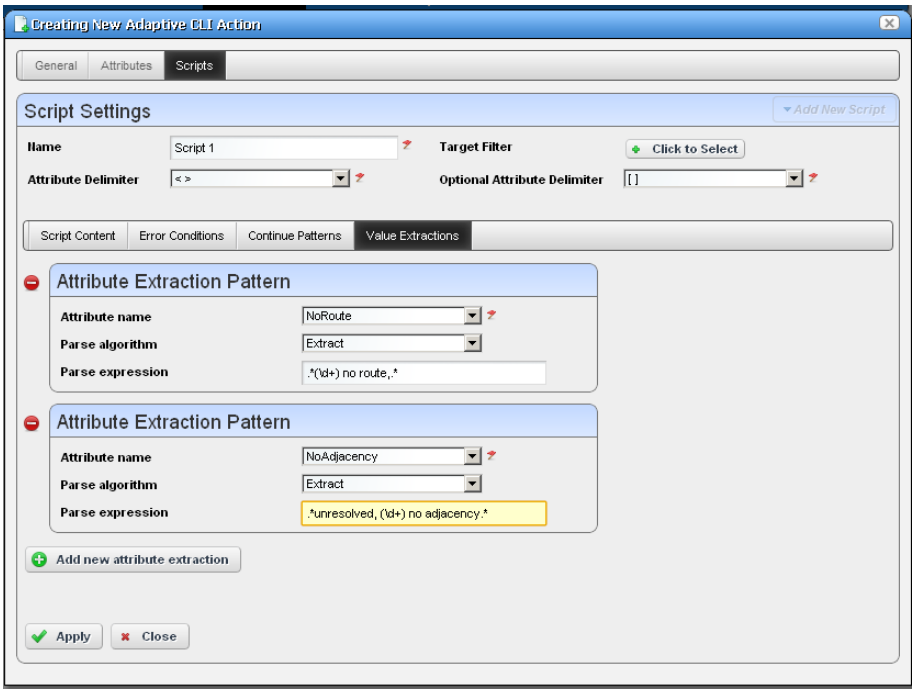
3 Create an attribute for `no_route,` too.

4 Create the script which contains the command you want to run. Notice the the attributes appear listed on the right panel. Do not refer to the attributes in the script as you would in a configuration script. The next step contains attribute references.



5 In the Value Extractions Tab click *Add new attribute extraction* and then pick the attribute. The Parse Expression is the RegEx that extracts the correct data. For `no_route` use this RegEx: `.*(\d+) no route,.*`

6 *Add* the next attribute. For `no_adjacency` use the RegEx: `.*unresolved, (\d+) no adjacency.*`



7 Apply and Save the ACLI.

8 Select the ACLI and execute it, selecting the devices you want to monitor.

The audit panel catalogs the progress of the job, and the Execution History snap panel in the expanded Actions portlet displays the execution, listing multiple executions by time and date. Right-click an execution listed, and select *Results* to see the results.

Create the Monitor

Follow these steps to monitor the Adaptive CLI created in the previous section.

1 Create a new monitor, select *Adaptive CLI* as the type.

2 Name the monitor, set the polling interval.

3 Select device(s) to monitor and then select the ACLI you just created. Notice that the attributes appear in the *input parameters* tab.

4 Under the Monitor Attributes tab, use the defaults.

5 Set any thresholds you like in the *Thresholds* node. This example monitors normal functionality so it includes no thresholds.

6 When you save the monitor it begins working and executes the ACLI every polling cycle, extracting the data.



How To:

Create a Monitor for an External Script

The following steps describe creating a monitor for an external command configured as an Adaptive CLI (ACLI).

Create the Adaptive CLI

1 Right click in the Actions portlet, and create a new *External Command* ACLI

2 Make a new attribute schema with attribute: Status (integer)

3 In Scripts, enter the following as Script Content:

```
perl "C:\[installation path] \owareapps\performance\scripts\
    http_test.pl"[_EquipmentManager_IP_Address]
```

The path that precedes the owareapps directory may differ if you have installed OpenManage Network Manager elsewhere, and by default on Linux.

Several Perl scripts appear in this performance\scripts directory by default. You can try others in addition to the http_test.pl script.

4 In the Value Extraction panel enter the following:

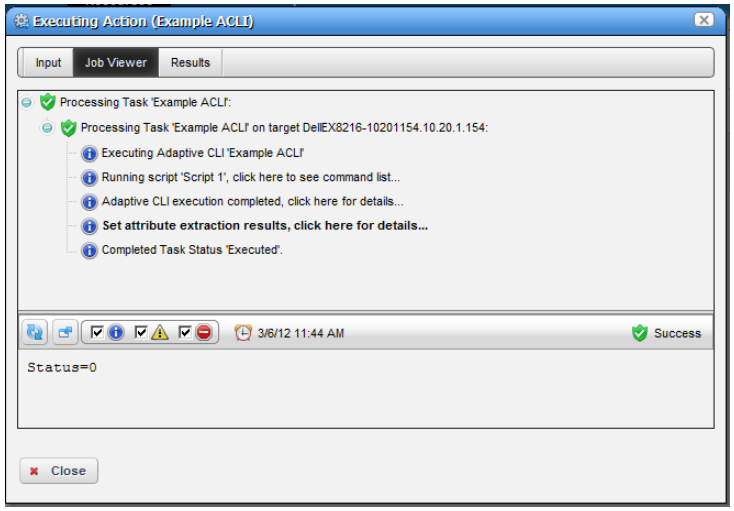
```
^\{(\d+)\}.*
```

5 Click Apply

6 Click Save

7 Right click and *Execute* the ACLI to test it.

8 Look in Job Viewer for the results.



Click *Set attribute extraction results, click here* to see the results appear in the bottom panel. Notice also that you must check informational messages for all these to appear, and that several additional sets of messages besides the extraction results appear.

Create a Monitor for the External Script Adaptive ACLI

Now that you have verified the script is working, you can create a monitor to see how this attribute is doing.

1 In the Monitors portlet, create a new ACLI Monitor

2 Uncheck *Update Network Status* (recommended since the ICMP monitor is already doing this)

3 In *Monitor Options* select your example monitor configured previously.

4 Confirm that *Monitor Attributes* displays the Status attribute configured previously.

5 In the *Conditions* tab of the Monitor Editor, create “Status Up” condition, with the severity of *Informational*, and check *Alert*.

6 Create a criterion which is Status = 0.

7 Save this condition

8 Create a new Condition called “Status Down”

9 The criterion is Status = 1

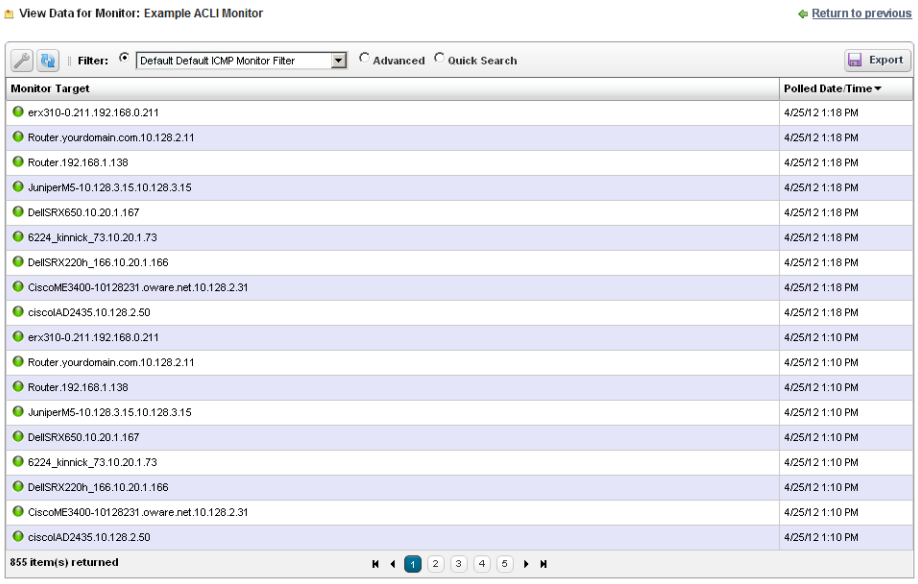
10 Apply and Save

11 Save your monitor

NOTICE

You may want to test your monitor, in which case, you may want to change the interval to 30 seconds.

12 Right-click to select View Monitor Data, and you can see the results of your efforts.



How To:

Create a Monitor Report

You can create reports based on your monitors. The following example creates a report based on How to: Create an SNMP Interface Monitor above.

1 Create a new Report Template by right-clicking the Report Templates portlet, selecting *New* > *Table Template*.

2 Name the report (here: Test SNMP Interface Report).

3 Select a source in the Source tab. Here: *Active Monitoring* > *SNMP Interfaces*.

4 Notice that the *Select your inventory columns* panel displays the attributes available based on your monitor selection.

5 Select *Available* columns and click the right arrow to move them to *Selected*. In this case we select SNMP Interfaces: Monitor Target, Polled Date / Time, ifInErrors.

6 Arrange the columns and fonts as you like in the *Layout* tab.

7 *Save* the template.

8 Right-click, and select *New* in the Reports portlet.

9 Enter a *Name* and *Title* for the report.

10 Notice that since this is the first report created since you made the Test SNMP Interface Report template, that it is the *Report Template* already selected.

11 Since the monitor already filters devices, we add no filter in the Report, although you could add one to further filter the monitored devices.

12 Test SNMP Interface Report should appear in the Reports portlet.

13 Right-click and select *Execute* (noticing that you can also schedule such reports, even repeatedly).

14 Click the magnifying glass to the right of the Report Completed message in My Alerts to see the report.

15 Hover your cursor over the lower right corner of the report to see a set of icons that let you expand, zoom out and in, save, or print the report.



How To:

Create a Monitor Target Report

Simliar to Monitor Reports, you can create reports based on the targets associated with your monitors. The following example creates a report based on How to: Create an SNMP Interface Monitor above.

1 Create a new Report Template by right-clicking the Report Templates portlet, selecting New > Table Template.

2 Name the report (here: Test SNMP Interface Targets Report).

3 Select a source in the Source tab. Here: Active Monitoring > SNMP InterfacesTargets (there should be two entity types for each monitor: one for the actual monitor data, and one for the targets).

4 Notice that the Select your inventory columns panel displays the attributes associated with the monitor targets. These attributes are the same for each monitor target entity type. This is unlike the monitor data entity types, where the list of available attributes is different for each monitor.

5 Select Available columns and click the right arrow to move them to Selected. In this case we select Monitor Target, Equipment, Availability, Last Polled, Enabled, Device Management State.

6 Arrange the columns and fonts as you like in the Layout tab.

7 Save the template.

8 Right-click, and select New in the Reports portlet.

9 Enter a Name and Title for the report.

10 Notice that since this is the first report created since you made the Test SNMP Interface Targets Report template, that it is the Report Template already selected.

11 Since the monitor already filters devices, we add no filter in the Report, although you could add one to further filter the target devices and/or subcomponents.

12 Test SNMP Interface Target Report should appear in the Reports portlet.

13 Right-click and select Execute (noticing that you can also schedule such reports, even repeatedly).

14 Click the magnifying glass to the right of the Report Completed message in My Alerts to see the report.

Monitor Options Type-Specific Panels

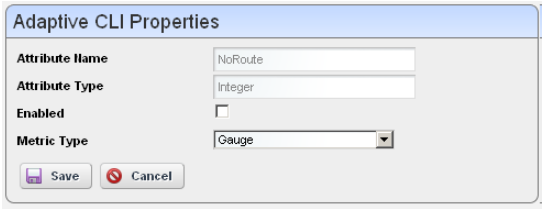
The following describes the panels associated with the following Monitor Options types.

- Adaptive CLI
- Cisco IPSLA
- Cisco Metro Ethernet SLA Monitors
- Cisco QoS Monitors
- ICMP
- Juniper CoS
- Juniper RPM
- Key Metrics
- ProScan
- SNMP
- SNMP Interfaces
- SNMP Table Monitor

Adaptive CLI

For this monitor, see How to Create an Adaptive CLI Monitor on page 189.

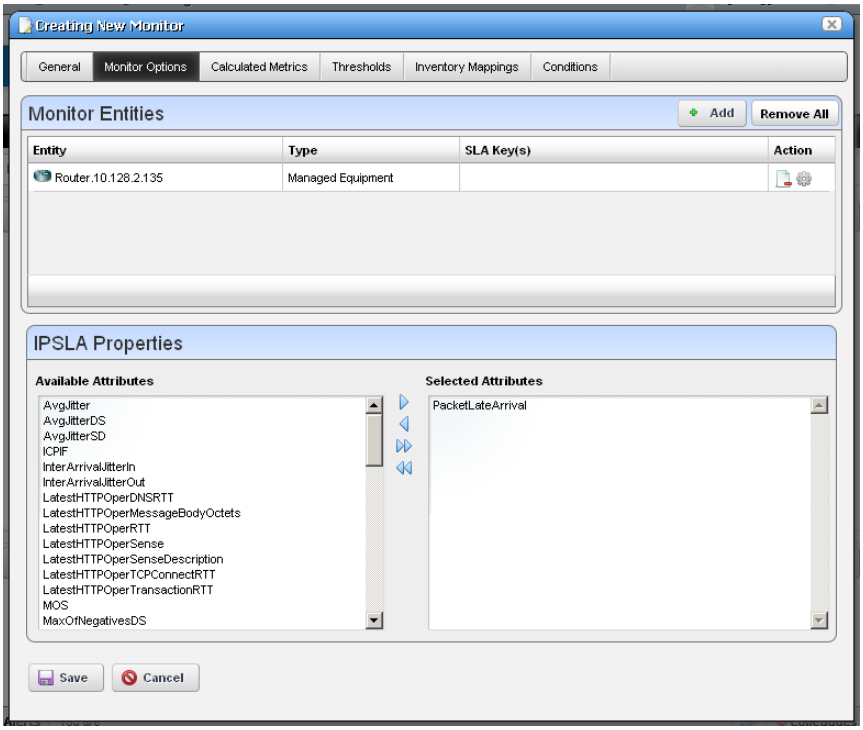
Select Monitor Entities in the top panel, and an Adaptive CLI to monitor at the top of the bottom panel. The *Input Parameters* for the Adaptive CLI appear in that tab, and you can edit the *Monitor Attributes* in that tab.



The *Name* and *Type*, and whether the attribute is *Enabled* appear in this editor. You can also select whether the attribute is a Counter, Gauge or Boolean. For Counter types, the monitor computes change from previous readings, and for Gauges it does not. Boolean attributes are either true or false

Cisco IPSLA

This screen configures options for Cisco IPSLA monitoring.



CAUTION:

Target equipment for this monitor must be an IPSLA transmitter, not an IPSLA responder.

Click to select from *Available Attributes* and use the arrows to move such attributes to *Selected Attributes* that you want to monitor.

NOTICE

This Monitor provides end-to-end service verification. Alarms appear in the Service Details Panel and service topology (Visualize). You must configure the monitor to emit availability events for this to occur.

IPSLA OIDS

The following are the object IDs for IPSLA, all found in CISCO-RTTMON-MIB

Monitor Attribute Name	Mib Attribute name	OID
NumOfPositvesDS	rttMonEchoAdminNumPackets	1.3.6.1.4.1.9.9.42.1.2.2.1.18
NumOfRTT	rttMonLatestJitterOperNumOfRTT	1.3.6.1.4.1.9.9.42.1.5.2.1.1
RTTSum	rttMonLatestJitterOperRTTSum	1.3.6.1.4.1.9.9.42.1.5.2.1.2
RTTSum2	rttMonLatestJitterOperRTTSum2	1.3.6.1.4.1.9.9.42.1.5.2.1.3
MinRTT	rttMonLatestJitterOperRTTMin	1.3.6.1.4.1.9.9.42.1.5.2.1.4
MaxRTT	rttMonLatestJitterOperRTTMax	1.3.6.1.4.1.9.9.42.1.5.2.1.5
MinOfPositivesSD	rttMonLatestJitterOperMinOfPositivesSD	1.3.6.1.4.1.9.9.42.1.5.2.1.6

Monitor Attribute Name	Mib Attribute name	OID
MaxOfPositvesSD	rttMonLatestJitterOperMaxOfPositivesSD	1.3.6.1.4.1.9.9.42.1.5.2.1.7
NumOfPositivesSD	rttMonLatestJitterOperNumOfPositivesSD	1.3.6.1.4.1.9.9.42.1.5.2.1.8
NumOfPositivesDS	rttMonLatestJitterOperSumOfPositivesSD	1.3.6.1.4.1.9.9.42.1.5.2.1.9
Sum2PositivesSD	rttMonLatestJitterOperSum2PositivesSD	1.3.6.1.4.1.9.9.42.1.5.2.1.10
MinOfNegativesSD	rttMonLatestJitterOperMinOfNegativesSD	1.3.6.1.4.1.9.9.42.1.5.2.1.11
MaxOfNegativesSD	rttMonLatestJitterOperMaxOfNegativesSD	1.3.6.1.4.1.9.9.42.1.5.2.1.12
NumOfNegativesSD	rttMonLatestJitterOperNumOfNegativesSD	1.3.6.1.4.1.9.9.42.1.5.2.1.13
SumOfNegativesSD	rttMonLatestJitterOperSumOfNegativesSD	1.3.6.1.4.1.9.9.42.1.5.2.1.14
Sum2NegativesSD	rttMonLatestJitterOperSum2NegativesSD	1.3.6.1.4.1.9.9.42.1.5.2.1.15
MinOfPositivesDS	rttMonLatestJitterOperMinOfPositivesDS	1.3.6.1.4.1.9.9.42.1.5.2.1.16
MaxOfPositivesDS	rttMonLatestJitterOperMaxOfPositivesDS	1.3.6.1.4.1.9.9.42.1.5.2.1.17
NumOfPositivesDS	rttMonLatestJitterOperNumOfPositivesDS	1.3.6.1.4.1.9.9.42.1.5.2.1.18
SumOfPositivesDS	rttMonLatestJitterOperSumOfPositivesDS	1.3.6.1.4.1.9.9.42.1.5.2.1.19
Sum2PositivesDS	rttMonLatestJitterOperSum2PositivesDS	1.3.6.1.4.1.9.9.42.1.5.2.1.20
MinOfNegativesDS	rttMonLatestJitterOperMinOfNegativesDS	1.3.6.1.4.1.9.9.42.1.5.2.1.21
MaxOfNegativesDS	rttMonLatestJitterOperMaxOfNegativesDS	1.3.6.1.4.1.9.9.42.1.5.2.1.22
NumOfNegativesDS	rttMonLatestJitterOperNumOfNegativesDS	1.3.6.1.4.1.9.9.42.1.5.2.1.23
SumOfNegativesDS	rttMonLatestJitterOperSumOfNegativesDS	1.3.6.1.4.1.9.9.42.1.5.2.1.24
Sum2NegativesDS	rttMonLatestJitterOperSum2NegativesDS	1.3.6.1.4.1.9.9.42.1.5.2.1.25
PacketLossSD	rttMonLatestJitterOperPacketLossSD	1.3.6.1.4.1.9.9.42.1.5.2.1.26
PacketLossDS	rttMonLatestJitterOperPacketLossDS	1.3.6.1.4.1.9.9.42.1.5.2.1.27
PacketOutOfSequence	rttMonLatestJitterOperPacketOutOfSequence	1.3.6.1.4.1.9.9.42.1.5.2.1.28
PacketMIA	rttMonLatestJitterOperPacketMIA	1.3.6.1.4.1.9.9.42.1.5.2.1.29

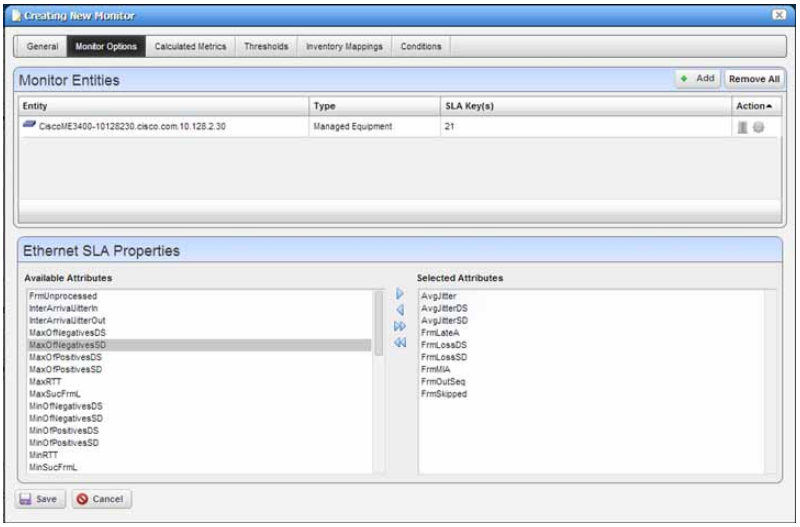
Monitor Attribute Name	Mib Attribute name	OID
PacketLateArrival	rttMonLatestJitterOperPacketLateArrival	1.3.6.1.4.1.9.9.42.1.5.2.1.30
OWSumSD	rttMonLatestJitterOperOWSumSD	1.3.6.1.4.1.9.9.42.1.5.2.1.33
OWSum2SD	rttMonLatestJitterOperOWSum2SD	1.3.6.1.4.1.9.9.42.1.5.2.1.34
OWMinSD	rttMonLatestJitterOperOWMinSD	1.3.6.1.4.1.9.9.42.1.5.2.1.35
OWMaxSD	rttMonLatestJitterOperOWMaxSD	1.3.6.1.4.1.9.9.42.1.5.2.1.36
OWSumDS	rttMonLatestJitterOperOWSumDS	1.3.6.1.4.1.9.9.42.1.5.2.1.37
OWSum2DS	rttMonLatestJitterOperOWSum2DS	1.3.6.1.4.1.9.9.42.1.5.2.1.38
OWMinDS	rttMonLatestJitterOperOWMinDS	1.3.6.1.4.1.9.9.42.1.5.2.1.39
OWMaxDS	rttMonLatestJitterOperOWMaxDS	1.3.6.1.4.1.9.9.42.1.5.2.1.40
NumOfOW	rttMonLatestJitterOperNumOfOW	1.3.6.1.4.1.9.9.42.1.5.2.1.41
MOS	rttMonLatestJitterOperMOS	1.3.6.1.4.1.9.9.42.1.5.2.1.42
ICPIF	rttMonLatestJitterOperICPIF	1.3.6.1.4.1.9.9.42.1.5.2.1.43
InterArrivalJitterOut	rttMonLatestJitterOperIAJOut	1.3.6.1.4.1.9.9.42.1.5.2.1.44
InterArrivalJitterIn	rttMonLatestJitterOperIAJIn	1.3.6.1.4.1.9.9.42.1.5.2.1.45
AvgJitter	rttMonLatestJitterOperAvgJitter	1.3.6.1.4.1.9.9.42.1.5.2.1.46
AvgJitterSD	rttMonLatestJitterOperAvgSDJ	1.3.6.1.4.1.9.9.42.1.5.2.1.47
AvgJitterDS	rttMonLatestJitterOperAvgDSJ	1.3.6.1.4.1.9.9.42.1.5.2.1.48
OWAvgSD	rttMonLatestJitterOperOWAvgSD	1.3.6.1.4.1.9.9.42.1.5.2.1.49
OWAvgDS	rttMonLatestJitterOperOWAvgDS	1.3.6.1.4.1.9.9.42.1.5.2.1.50
LatestHTTPOperRT	rttMonLatestHTTPOperRTT	1.3.6.1.4.1.9.9.42.1.5.1.1.1
LatestHTTPOperDNSRTT	rttMonLatestHTTPOperDNSRTT	1.3.6.1.4.1.9.9.42.1.5.1.1.2
LatestHTTPOperTCPConnectRTT	rttMonLatestHTTPOperTCPConnectRTT	1.3.6.1.4.1.9.9.42.1.5.1.1.3
LatestHTTPOperTransactionRTT	rttMonLatestHTTPOperTransactionRTT	1.3.6.1.4.1.9.9.42.1.5.1.1.4
LatestHTTPOperMessageBodyOctets	rttMonLatestHTTPOperMessageBodyOctets	1.3.6.1.4.1.9.9.42.1.5.1.1.5
LatestHTTPOperSense	rttMonLatestHTTPOperSense	1.3.6.1.4.1.9.9.42.1.5.1.1.6

Monitor Attribute Name	Mib Attribute name	OID
LatestHTTPErrorSenseDescription	rttMonLatestHTTPErrorSenseDescription	1.3.6.1.4.1.9.9.42.1.5.1.1.7
LatestRttOperCompletionTime	rttMonLatestRttOperCompletionTime	1.3.6.1.4.1.9.9.42.1.2.10.1.1

Cisco Metro Ethernet SLA Monitors

This monitor Cisco's CISCO-IPSLA-ETHERNET-MIB. It collects performance metrics against individual RTT probe operations for the target device. This monitor works like the existing Cisco IPSLA monitor for the CISCO-RTTMON-MIB. It indexes statistics using the probe index as defined in the rttMonCtrlAdminTable in the CISCO-RTTMON-MIB. The Ethernet jitter probes have a rttMonCtrlAdminRttType of ethernetJitter.

OpenManage Network Manager does not provide configuring of Ethernet jitter SLA operations. Information about configuring CFM can be found in the following documents found on the Cisco web site: *Configuring Ethernet CFM and OAM* and *Configuring IP SLAs for Metro-Ethernet*.

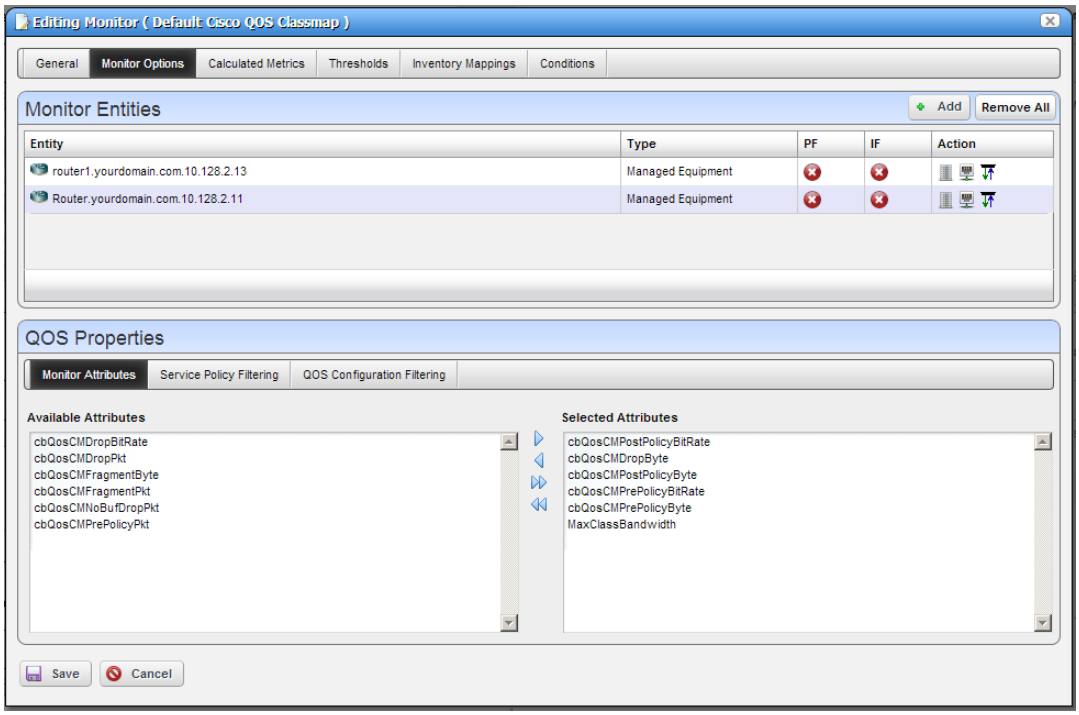


To create a Cisco Metro Ethernet monitor, select New Monitor > Cisco Ethernet SLA from the right-click menu in the Resource Monitors portlet. The Monitor Options screen lets you configure monitored attributes and devices. As with the IPSLA monitor, you can select either equipment groups or individual managed equipment objects. If you select a managed equipment object you can click on the gear icon in the Action column to see a list of the Ethernet Jitter SLA probe IDs configured for that device and select specific probes which then appear in the SLA Key(s) column. Without such a selection, the monitor tracks all Ethernet Jitter SLA probes for the device.

The Ethernet SLA Properties panel allows selection of the specific attributes you wish to collect data on. The attributes correspond directly to the oids in the ipslaEtherJitterAggStatsTable in the ipslaEthernetStats section of the CISCO-IPSLA-ETHERNET-MIB.

Cisco QoS Monitors

This monitors values for Cisco QoS from the Cisco Class-Based QOS MIB. The following screenshots come from the Class Map monitor, but OpenManage Network Manager's Cisco QoS monitoring capabilities include more than just this monitor. See Additional QoS Monitors on page 202.



Service Policies

A Service Policy is a policy map attached to a logical interface. Because a policy map can also be a part of the hierarchical structure (inside a classmap), OpenManage Network Manager considers only a policy map directly attached to a logical interface as a service policy.

Class Map—A user-defined traffic class that contains one or many match statements that classify packets into different categories.

Match Statement—Specifies specific match criteria to identify packets for classification purposes. Match statements exist within a class map.

Policy Map—A user-defined policy that associates QoS actions to the user-defined traffic class - ClassMap.

Qos Actions—These include: Queueing, Random Detect (WRED), Traffic Shaping, Police, Set (Packet Marking), Compression (IP header), Account (C3pl).

See Additional QoS Monitors on page 202 for attributes you can monitor related to these.

Monitor Entitles

Select the equipment to monitor in this screen. Notice the *PF* and *IF* columns that indicate whether a port filter or interface filter is active to further limit what parts of the selected device is monitored. Delete the device or configure port and interface filters with the icons to the right of listed equipment.

QOS Properties - Monitored Attributes

This panel lets you select attributes monitored with right/left selection arrows. Move the desired attributes from the *Available* to the *Selected* side of this panel. Notice that, by default, you can monitor two additional calculated attributes. You can also edit the monitor to create additional calculated attributes, which would also appear here.

NOTE:

If you change the bandwidth (speed) on an port/interface, you must resync the device to update the port speed in OpenManage Network Manager. You must refresh targets on any QOS monitor after resync for the application to reflect the correct MaxClassBandwidth value. See also Bandwidth Calculation on page 216.

Additional QoS Monitors

The sections below list the monitored attributes for possible Monitor types that include the following:

- Qos Class Map Monitor
- Qos Match Statement Monitor
- Qos Police Monitor
- Qos Queuing Monitor
- Qos Traffic Shaping Monitor
- Qos RED Monitor
- Qos IPHC Monitor
- Qos Packet Marking Monitor
- QoS Police Monitor
- Qos Estimate Bandwidth Monitor
- QoS C3pl Account Monitor

Qos Class Map Monitor

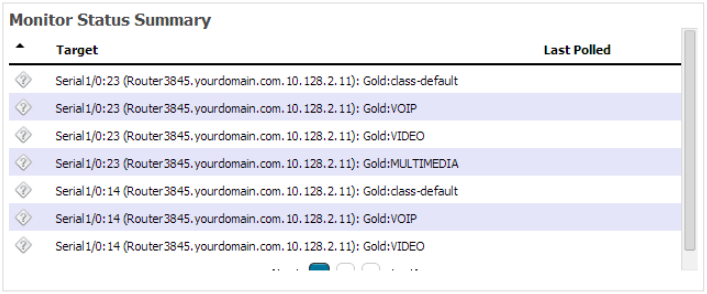
Qos Class Map Monitor collects metrics from the cbQosCMStatsTable. This table specifies ClassMap related Statistical information.

Available Metrics:

```
DropBitRate
PrePolicyPkt
PrePolicyByte
PrePolicyBitRate
PostPolicyByte
PostPolicyBitRate
DropPkt
DropByte
NoBufDropPkt
FragmentPkt
FragmentByte
```

Target Summary Pattern

This pattern appears in the expanded Resource Monitors portlet when you select the monitor in the top panel




```
<PolicyMapName> : <Name>
```

Qos Match Statement Monitor

Qos Match Statement Monitor collects metrics from the cbQosMatchStmtStatsTable. This table specifies Match Statement related statistical information.

Available Metrics

```
PrePolicyPkt
PrePolicyByte
PrePolicyBitRate
```

Target Summary Pattern

This pattern appears in the expanded Resource Monitors portlet when you select the monitor in the top panel

```
<PolicyMapName> : <Name> : <StmtName>
```

Qos Police Monitor

Qos Police Monitor collects metrics from the cbQosPoliceStatsTable. This table specifies Police Action related statistical information.

Available Metrics

```
ConformedPkt
ConformedByte
ConformedBitRate
ExceededPkt
ExceededByte
ExceededBitRate
ViolatedPkt
ViolatedByte
ViolatedBitRate
```

Target Summary Pattern

This pattern appears in the expanded Resource Monitors portlet when you select the monitor in the top panel

```
<PolicyMapName> : <CMName> : <CfgRate>
```

Qos Queuing Monitor

Qos Queuing Monitor collects metrics from the cbQosQueueingStatsTable. This table specifies Queueing Action-related statistical information.

Available Metrics

```
CurrentQDepth
MaxQDepth
DiscardByte
DiscardPkt
```

QoS Configuration Filtering Attributes

```
CfgBandwidth - specified in kbps or percentage
CfgBandwidthUnits - enumeration
```

Target Summary Pattern

This pattern appears in the expanded Resource Monitors portlet when you select the monitor in the top panel

```
<PolicyMapName> : <CMName> : <CfgBandwidth>
```

Qos Traffic Shaping Monitor

Qos Traffic Shaping Monitor collects metrics from the cbQosTSStatsTable. This table specifies traffic-shaping Action related statistical information.

Available Metrics

```
DelayedByte
DelayedPkt
DropByte
DropPkt
Active
QSize
```

Target Summary Pattern

This pattern appears in the expanded Resource Monitors portlet when you select the monitor in the top panel

```
<PolicyMapName> : <CMName>  : <TSCfgRate>
```

Qos RED Monitor

Qos RED Monitor collects metrics from the cbQosREDClassStatsTable. This table specifies per Precedence WRED (wait random early detection) Action-related statistical information.

Available Metrics

```
RandomDropPkt
RandomDropByte
TailDropPkt
TailDropByte
TransmitPkt
TransmitByte
ECNMarkPkt
ECNMarkByte
MeanQSizeUnits
MeanQSize
```

Target Summary Pattern

This pattern appears in the expanded Resource Monitors portlet when you select the monitor in the top panel

```
<PolicyMapName> : <CMName> : < CfgDscpPrec >
```

Qos IPHC Monitor

Qos IPHC Monitor collects metrics from the cbQosIPHCStatsTable. This table specifies IP Header Compression statistical information.

Available Metrics

```
RtpSentPkt
RtpCmprsOutPkt
RtpSavedByte
RtpSentByte
RtpSentByteRate
TcpSentPkt
TcpCmprsOutPkt
TcpSavedByte
TcpSentByte
TcpSentByteRate
RtpFullHdrSentPkt
TcpFullHdrSentPkt
```

Target Summary Pattern

This pattern appears in the expanded Resource Monitors portlet when you select the monitor in the top panel

```
<cbQosPolicyMapName> : <cbQosCMName> : <CfgOption>
```

Qos Packet Marking Monitor

Qos Packet Marking Monitor collects metrics from the cbQosSetStatsTable. This table specifies packet marking statistical information.

Available Metrics

```
DscpPkt
PrecedencePkt
QosGroupPkt
FrDePkt
AtmClpPkt
L2CosPkt
MplsExpImpositionPkt
DiscardClassPkt
MplsExpTopMostPkt
SrpPriorityPkt
FrFecnBecnPkt
DscpTunnelPkt
PrecedenceTunnelPkt
```

Target Summary Pattern

This pattern appears in the expanded Resource Monitors portlet when you select the monitor in the top panel

```
<cbQosPolicyMapName> : <cbQosCMName> : <CfgFeature>
```

QoS Police Monitor

Qos Police Monitor collects metrics from the cbQosPoliceColorStatsTable. This table specifies Police Action-related statistical information for two rate color aware marker.

Available Metrics

```
ConformedBitRate
ConfirmedByte
ConformedPkt
ExceededBitRate
ExceededByte
ExceededPkt
ViolatedBitRate
ViolatedByte
ViolatedPkt
```

Target Summary Pattern

This pattern appears in the expanded Resource Monitors portlet when you select the monitor in the top panel

```
<cbQosPolicyMapName> : <cbQosCMName> : <cbQosPoliceCfgRate>
```

Qos Estimate Bandwidth Monitor

Qos Estimate Bandwidth Monitor will collect metrics from the cbQosEBStatsTable. This table specifies Estimate Bandwidth related statistical information.

Available Metrics

```
StatsCorvilEBValue
StatsCorvilEBStatus
StatsCorvilCTD
```

Target Summary Pattern

This pattern appears in the expanded Resource Monitors portlet when you select the monitor in the top panel

```
<cbQosPolicyMapName> : <cbQosCMName> : <???>
```

QoS C3pl Account Monitor

Qos C3pl Account Monitor collects metrics from the cbQosC3plAccountStatsTable. This table specifies C3pl Account Action-related statistics information.

Available Metrics

```
cbQosC3plAccountDropPkt
cbQosC3plAccountDropByte
cbQosC3plAccountTailDropPkt
cbQosC3plAccountTailDropByte
```

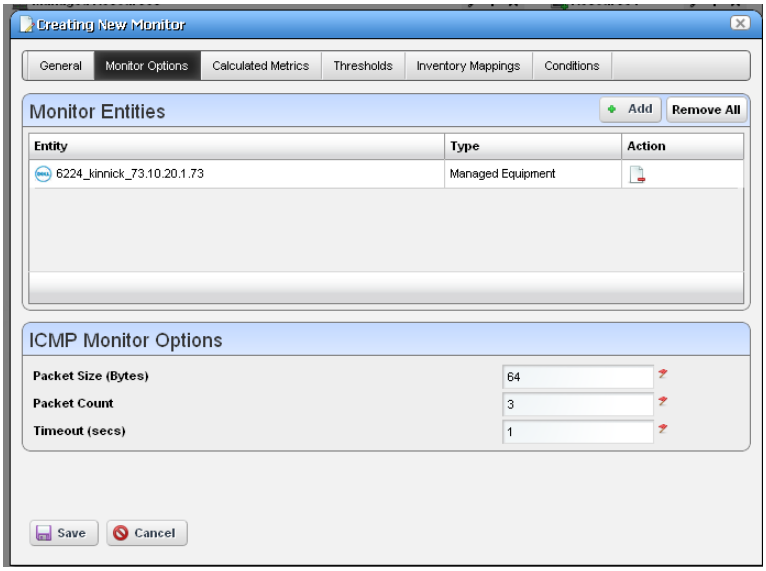
Target Summary Pattern

This pattern appears in the expanded Resource Monitors portlet when you select the monitor in the top panel

```
<cbQosPolicyMapName> : <cbQosCMName> : <cbQosC3plAccountFeatureType>
```

ICMP

The ICMP Monitor Options panel contains the following properties:



Packet Size—Size of packet for ICMP transmission

Packet Count—Number of packets to send.

Timeout—Number of seconds without a response before a timeout is issued

The ICMP Entity Panel lets you select resource groups and Resource manager objects. Clicking *Add* button displays a selector panel for these.

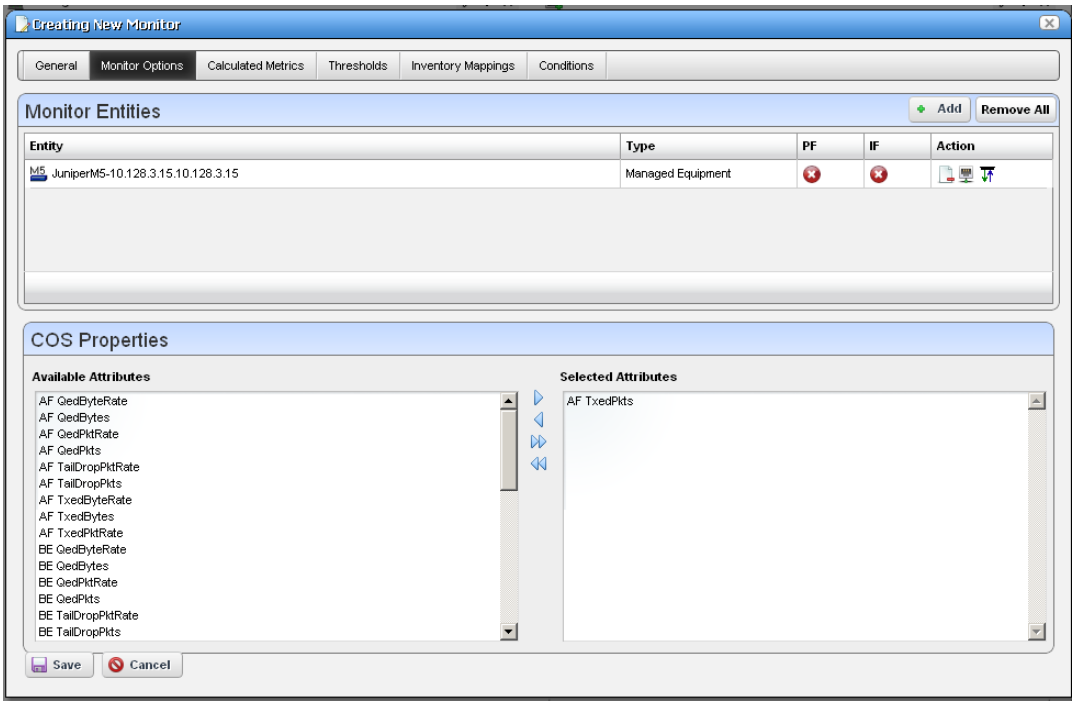
Select the type of entity you want to add, then select any desired filter attributes, then click *Apply Filter*. Select from the entities that appear and add them to the monitor.

NOTE:

Migrating from previous versions updates the Network Status check box to true and redeploys the monitor.

Juniper CoS

This (optional) monitor uses the fields described below and lets you track CoS attributes for Juniper equipment. It appears only on systems with a Juniper device driver installed.



Monitor Entities

Click *Add* to configure monitored devices in a subsequent selector screen. This is the typical selector with a filter to help you find discovered devices.

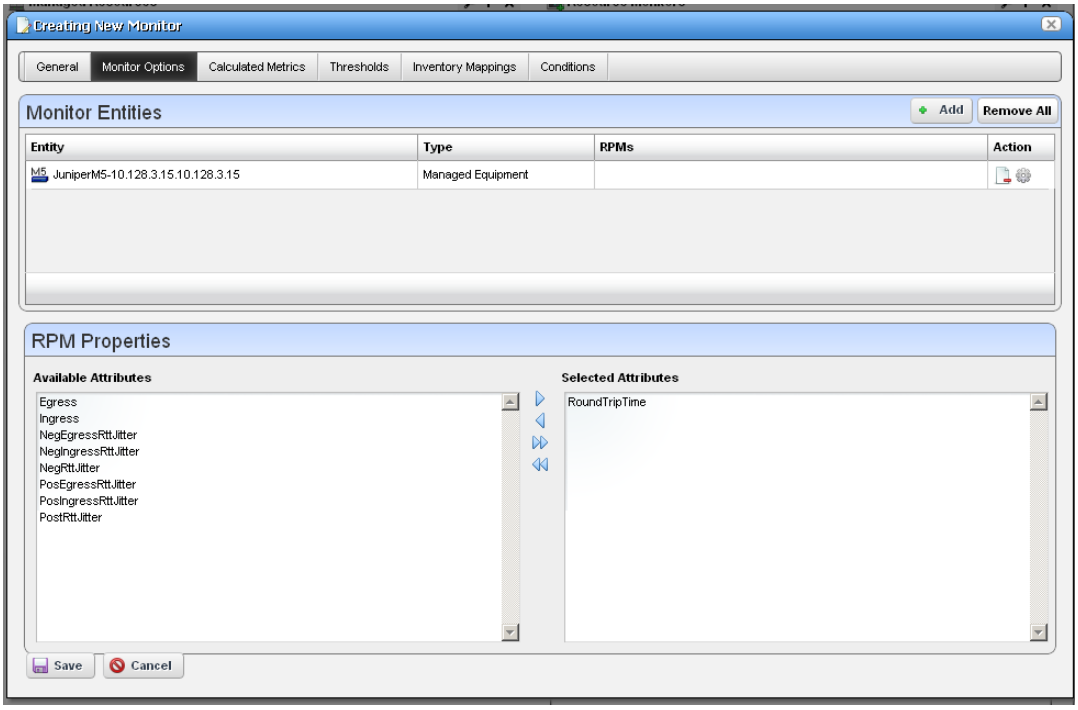
At the right you can see *PF* (Port Filter) and *IF* (Interface Filter) columns, which display green icons if such filters are active. Click the *Configure Port / Interface Filter* icon at the far right to configure such filters. These contain the standard filtering mechanism visible throughout OpenManage Network Manager. (See Defining Advanced Filters on page 86, for example). Notice that for port and interface filters, the editor also lets you delete the filter. The *Delete* button on the right of listed Monitor Entities lets you delete equipment.

COS Properties

Click to select *Available Attributes*, and use the arrows between columns to move these to the *Selected Attributes* column to select the monitored CoS properties.

Juniper RPM

This (optional) monitor uses the fields described below and lets you track RPM attributes for Juniper equipment. It appears only on systems with a Juniper device driver installed.



Monitor Entities

Click *Add* to configure monitored devices in a subsequent selector screen. This is the typical selector with a filter to help you find discovered devices.

At the right you can see the *RPMs* column. This displays information about RPM probes. Click the *Configure RPM Probes* icon (a gear) at the far right to select and configure such probes. The *Delete* button on the right of listed Monitor Entities lets you delete equipment and probe combinations.

RPM Properties

Click to select *Available Attributes*, and use the arrows between columns to move these to the *Selected Attributes* column to select the monitored RPM properties.

These monitors collect data for all tests for the selected probe(s), and collect only attributes assigned to them. If all attributes are assigned in the monitor, but only a handful of actual attributes are being tested, then the monitor collects only data from attributes running tests.

For example, if you select Egress to monitor, and tests occur for Egress, then the monitor collects Egress. However, if you select all attributes, and only Egress and PostRttJitter are tested, and the monitor collects only Egress and PostRttJitter.

Another example: If you select all attributes for the monitor, then slowly add more tests and attributes on the device, the monitor picks up these changed attributes as you add them to the tests.

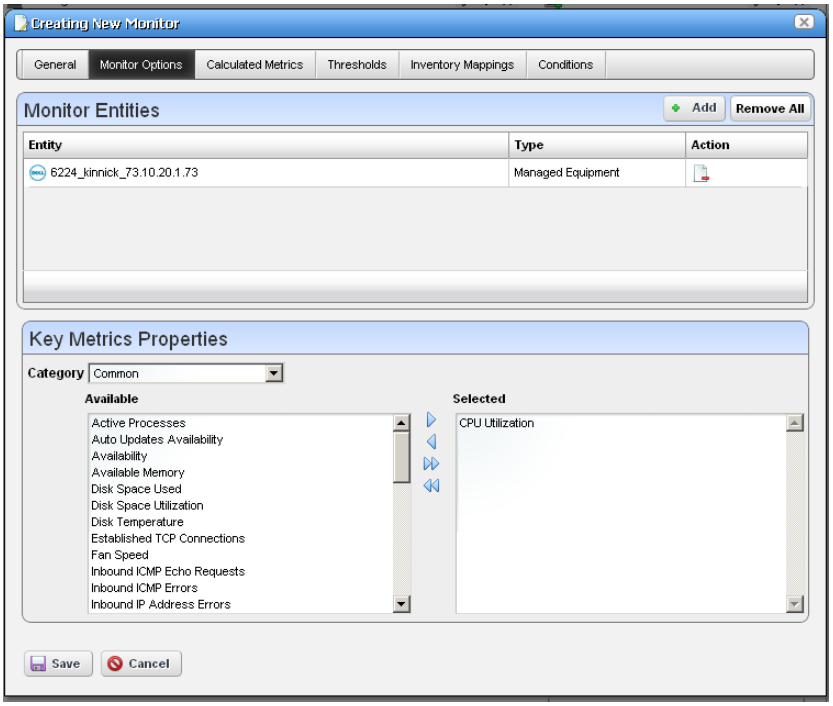
The default refresh rate is 30 minutes, but you can configure the refresh by overriding the attribute pm.monitor.rpm.refresh_rate. This property determines how often the monitor fetches the list of tests and attributes for the probe. Disable/Enable-ing the monitor also refreshes the list. The monitor can stay up to date with the device without much user intervention.

You can also change the attribute names (like Egress) too through the `pmmsgs.properties` file. Search for RPM and modify the nine attribute names. Remember, best practice is to override properties as described in Overriding Properties on page 71.

Click *Save* to preserve your edits, or *Cancel* to abandon them.

Key Metrics

The Key Metrics Properties panel contains a list of key metrics you can add to the monitor. They are grouped by category.

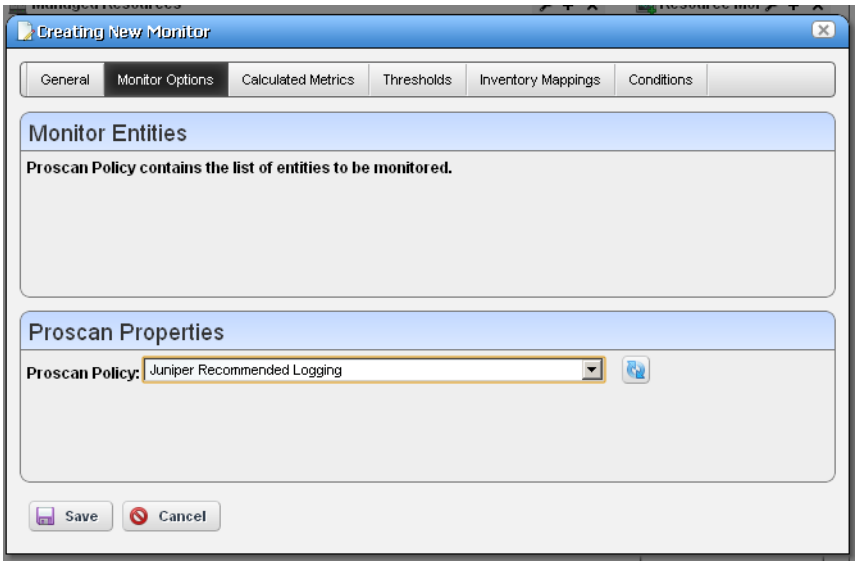


The Monitor Entities Panel lets you select equipment group and equipment manager objects (as described in ICMP on page 207, above).

The Key Metrics Properties panel at the bottom of this screen uses a pre-defined list of key metrics. It does not check if the key metrics selected are supported by the devices and groups selected in the monitor.

ProScan

In this screen, you simply select the Proscan policy to monitor. In the Thresholds tab, you can set thresholds for both in and out of compliance numbers.



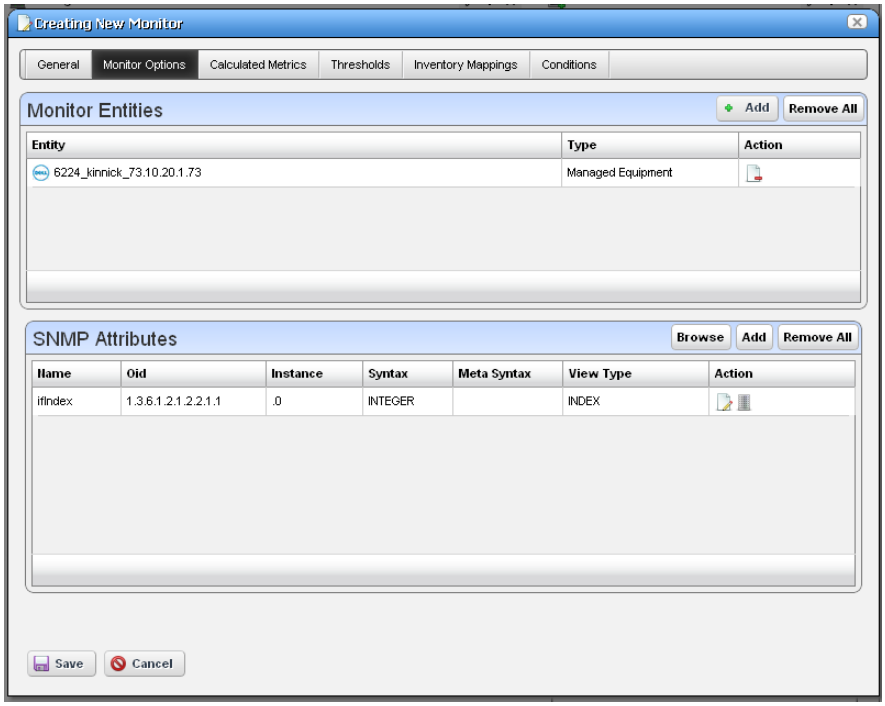
The Proscan policy contains the target network assets.

Execute the Proscan only *after* creating the monitor. The Proscan monitor displays data when you create it and its supporting Proscan policy in the following order:

1. Create Proscan policy X that has explicit targets.
2. Create a Proscan monitor referring to Proscan policy X, and modify polling to the desired interval.
3. Execute Proscan X.

SNMP

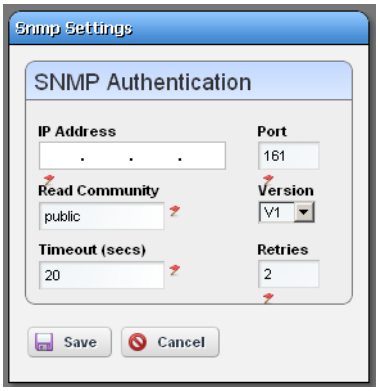
The SNMP attributes panel lets you specify which SNMP attributes are to be monitored.



You can specify the SNMP attributes the following ways:

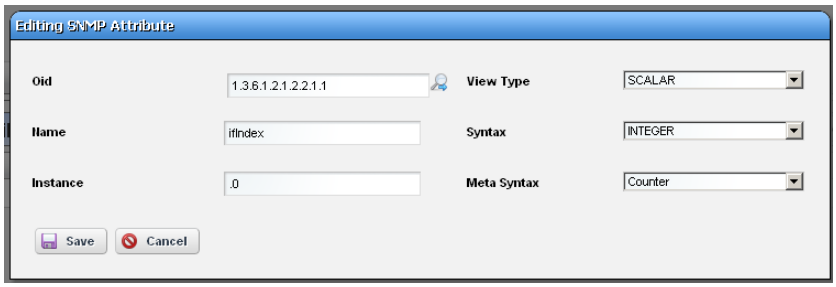
- With the SNMP browser, or
- Entering the SNMP attribute properties explicitly.

The *Browse* button launches the SNMP MIB browser. (See MIB Browser Tool on page 550) You can also click the *Device Results* tab to open an SNMP authentication screen and log into any device you specify, even undiscovered devices. Specify the IP address, SNMP Read Community, port, SNMP version, timeout and retries.



Click on the desired SNMP nodes and then click on the *Add Selection* button to add an SNMP attribute. When done selecting, click the *Done* button to add selected attributes to the monitor or *Cancel* to abandon the operation and close the browser.

The Add and Edit buttons in the SNMP attribute panel launch the SNMP Attribute editor.



This panel contains the following properties:

Oid—The object identifier for this attribute

Name—This attribute's name

Instance—SNMP instance. 0 for scalar or the ifIndex value for an SNMP column.

View Type—*Scalar* or *Column*.

Syntax—*Integer*, *Boolean*, *DisplayString*, and so on.

Meta Syntax—*Counter*, *Gauge*, and so on.

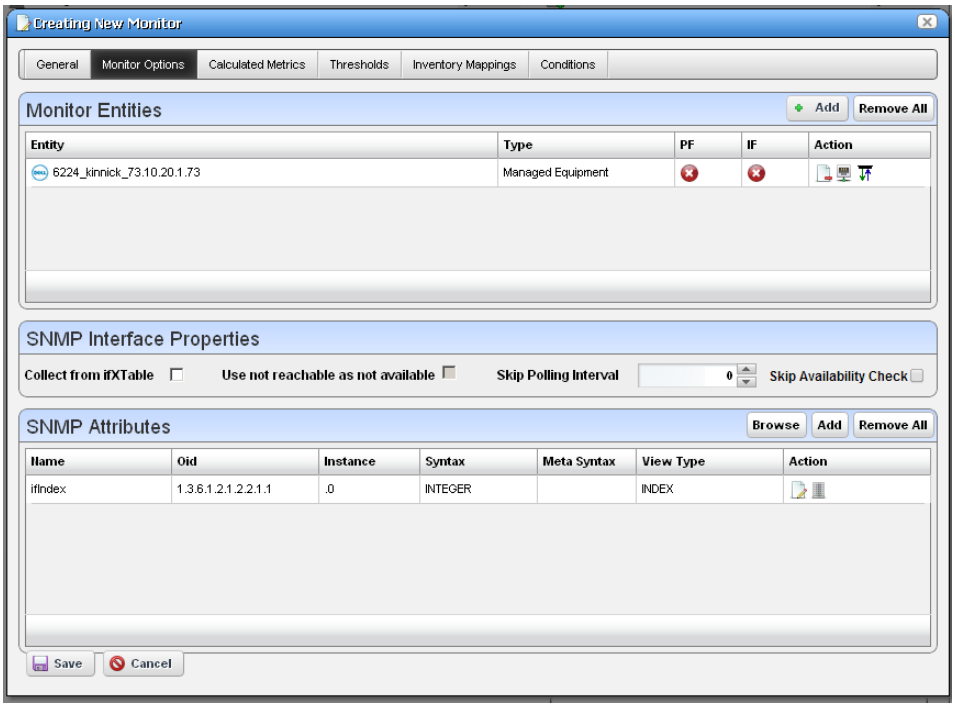
If you type in an OID and click the search button next to the OID field, the browser searches the MIB for the OID and fills in the other values if it finds the OID.

NOTE:

For all counter types, the polled data stored in database reflect the changes between two polled data points from an SNMP table.

SNMP Interfaces

The SNMP Interface Monitor Entity editor supports the following entity types: group, equipment manager, port and interface. It also supports port and interface filters on groups and equipment manager objects.



If you check the *Collect from ifXTable* checkbox, then OpenManage Network Manager attempts to fetch attributes from the ifXTable. These attributes are ifHighSpeed, ifHCInOctets, ifHCInUcastPkts, ifHCOutOctets and ifHCOutUcastPkts. If any of these attributes are not available, then it fetches from ifTable.

If an interface does not support ifxTable, SNMP get typically retrieves an error and OpenManage Network Manager uses the ifTable instead. Some ATM ports do not send errors from the ifxTable oids, so OpenManage Network Manager also uses the ifTable values if ifHighSpeed is 0.

NOTE:

The SNMP V1 protocol does not support 64bit counters located in ifXtable. This means OpenManage Network Manager monitors only collect performance data from ifTable when a device is discovered using the SNMP V1 protocol. Best practice: Discover devices using snmpV2c or snmpV3 protocols to collect performance data located in ifXtable.

Even with this checked, OpenManage Network Manager defaulting to 32-bit counters if 64-bit is not available.

OpenManage Network Manager now supports multiple indexes in the SNMP Interface monitor. Specify them in the instance field, separated by dots. For `sfpTxPowerValue 1.3.6.1.4.1.28458.7.2.4.6.7.1.22.Y.Z`, where `Y` is the slot and `Z` is the @ifindex, specify `@slotNumber.@ifIndex` as the instance. You can also specify a constant string. For `sonetLineIntervalUASs 1.3.6.1.2.1.10.39.1.3.2.1.5. X.16` Where `X` is the `@ifindex` and `16` is the last record, specify `@ifIndex.16`.

The variable name following the "@" must correspond to an attribute in the port or interface bean.

When determining the “not available” status of a device, SNMP AdminStatus and OperationalStatus messages both have to indicate a device is Available before a monitor determines it is available.

Certain devices that do not support ifTable availability indicators. For the sake of these devices, a *Skip availability check* checkbox appears.

The *Skip Polling Interval* configures skipped availability checks when polling, so you can check availability, for example, every fourth polling interval (skipping three). This helps the monitor avoid flutter artifacts

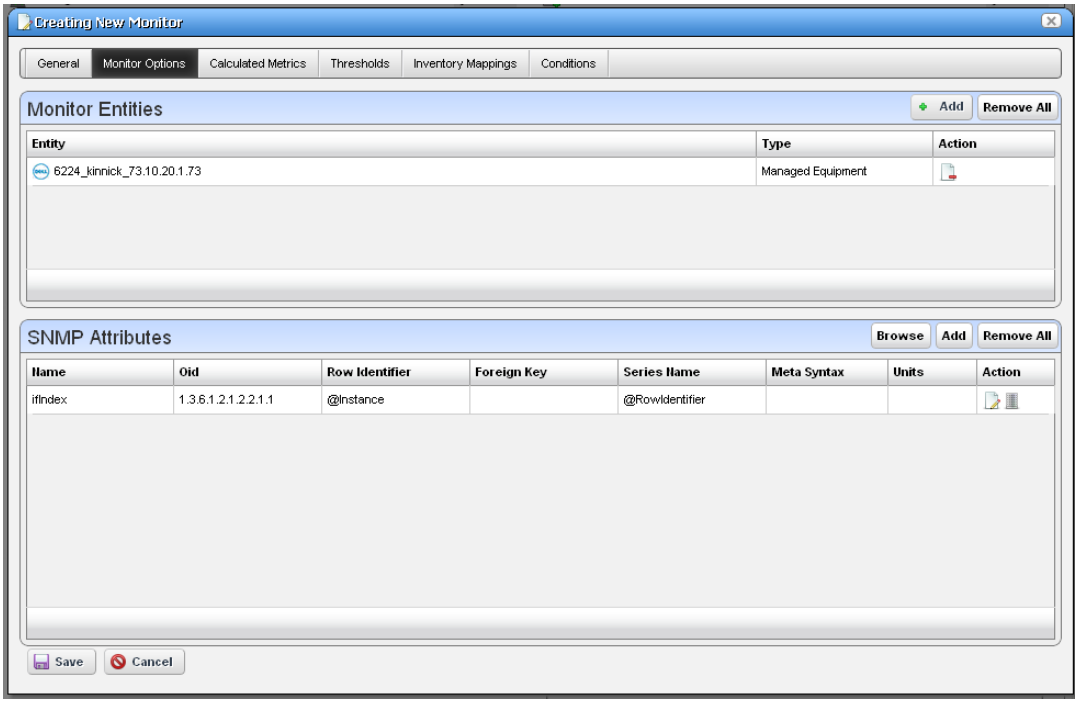
The PF and IF table columns indicate if a port filter or interface filter is configured for the entity. Click the icons on the right side of the list of Monitor Entities to configure filters. Clicking these buttons displays an interface configuration panel.

This panel lets you specify filter attributes for the port or interface filters you want to monitor. For example, if you select a device but only want to monitor active interfaces created by a particular user, then these filters do the job.

The SNMP Attributes panel is the same as described in SNMP on page 212.

SNMP Table Monitor

This panel appears if you are editing an SNMP Table monitor. The application stores not absolute numbers from counters but the counter’s change since its last measurement.



Columns include the SNMP Attribute Name, OID, Row Identifier, Foreign Key, Series Name, Meta Syntax, Units, and Action.

NOTICE

If you select one of the 64-bit counters in ifXTable, make sure the Meta Syntax is 64-bit.

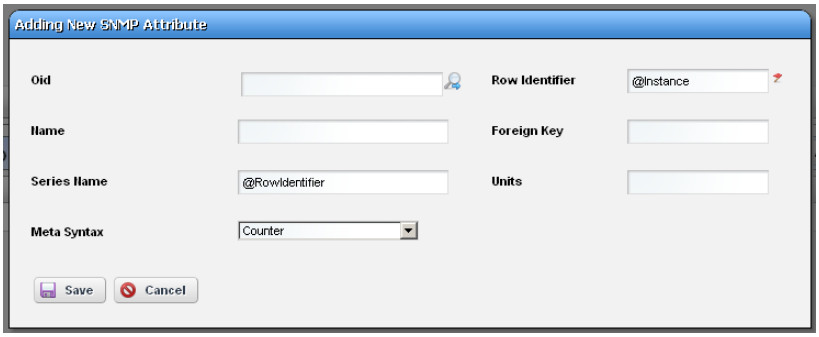
Clicking the *Add* or the *Edit* button to the right opens either a MIB Browser where you can retrieve these attributes, or an Add / Edit SNMP Attributes editor at the bottom of the screen, See the following sections for details.

MIB Browser

This lets you select attributes to monitor as described in MIB Browser Tool on page 550. The SNMP table monitor lets you pick a table column, not the entire table.

Add / Edit SNMP Attributes

This screen lets you specify individual attributes.



It has the following fields:

Oid— A field where you can enter the object identifier. This also has an integrated search function. Click the magnifying glass icon on the right to activate it. A successful search populates the rest of the fields for the object identifier.

Row Identifier—This mandatory field defaults to @instance (The OID instance).

Name—The text identifier for the OID

Foreign Key—Enter the foreign key, if any.

Series Name—This defaults to @RowIdentifier.

Units—Enter the units of measurement.

Meta Syntax—Further refine the variable type with the pick list. For example, you can select *Counter*32 (a 32-bit counter). For Counter types, the monitor computes change from previous readings, and for Gauges it does not.

NOTE:

If a message appears saying: "Device fault: Return packet too big" in the Monitor Status Summary, then you have selected too many SNMP attributes to poll in a single request. Please modify your monitor to request smaller numbers of attributes

Bandwidth Calculation

Cisco devices running IOS or IOS-XR can calculate bandwidth. To support this functionality, all ports and interfaces now have four new filterable attributes:

- Ingress Bandwidth (the ingress bandwidth in bps)
- Ingress Bandwidth Type (the type of calculation used to determine the ingress bandwidth)
- Egress Bandwidth (the egress bandwidth in bps), and
- Egress Bandwidth Type (the type of calculation used to determine the egress bandwidth).

Types of Bandwidth Calculation

The ways to arrive at a bandwidth number appear here in order, from highest priority to lowest priority. If OpenManage Network Manager can calculate bandwidth in more than one way for a particular port/interface, it uses the highest priority calculation type.

NOTE:

If a port or interface's Administrative State is not Up, its bandwidth will always be 0, regardless of the calculation type!

CONFIGURED—This means OpenManage Network Manager has a QoS policy configured directly against this port or interface. For example: a policer, shaper, or queuing policy. Policies applied to *input* affect the ingress bandwidth, *output* affect the egress bandwidth.

TRUNK AGGREGATION—This calculation means a port is in trunking mode and calculates its bandwidth from its access ports. Essentially, if a trunk shares a VLAN with any access port, that access port adds its bandwidth values to the trunk port's totals. This reverses ingress and egress values. The total ingress bandwidth of the access ports becomes the egress bandwidth of the trunk port, and the total egress bandwidth of the access ports becomes the ingress bandwidth of the trunk port. If a port in this configuration is no longer in trunking mode, it reverts to UNCONFIGURED.

INTERFACE AGGREGATION—If a port or interface has sub-interfaces, the total bandwidth of the parent is the sum of the bandwidth of its children. For example: If GigabitEthernet0/1 has four subinterfaces GigabitEthernet0/1.1, GigabitEthernet0/1.5, GigabitEthernet0/1.8 and GigabitEthernet0/1.9 and each sub-interface has bandwidth of 1G, the total bandwidth of GigabitEthernet0/1 will be 4G.

Unlike trunk aggregation, this does not reverse ingress and egress. The total ingress of the children becomes the total ingress of the parent, and the total egress of the children becomes the total egress of the parent. If a port or interface in this configuration loses all of its children (i.e. the interfaces all get deleted), it reverts to UNCONFIGURED.

ASSOCIATION—If a port is currently UNCONFIGURED and has a physical link to another port that isn't UNCONFIGURED, it takes the bandwidth of the linked port. This reverses Ingress and Egress—the linked port's ingress becomes the other port's egress and vice-versa. If someone deletes the link, the port reverts to UNCONFIGURED.

UNCONFIGURED—The default setting for bandwidth. This sets the ingress and egress bandwidth of a port or interface to the IfSpeed of the port. This means a 10G port with an IfSpeed of 10G registers an Ingress and Egress Bandwidth setting of 10G.

Triggering Bandwidth Calculations

On resync, OpenManage Network Manager's rules check for configured QoS policies and update the port and interface bandwidth as needed (the CONFIGURED bandwidth calculation type). OpenManage Network Manager adds any ports and interfaces registering a change in their bandwidth values (or any newly-created ports and interfaces, as in initial discovery) to a list to be processed after the resync is over. OpenManage Network Manager also queues the device for recalculation of TRUNK AGGREGATION every time it collects VLAN data (for example, during resync or during network data collection).

After the resync finishes, the OpenManage Network Manager bandwidth processor processes the list of ports and interfaces whose bandwidth values changed and re-check its calculations to see if INTERFACE AGGREGATION or ASSOCIATION calculation types are applicable, and then calculate them if necessary.

Link creation, modification or deletion also trigger recalculations of ASSOCIATION calculation type for the endpoints of the link in question.

OpenManage Network Manager adds any ports/interfaces that change in the bandwidth processor back to the processor, so that changes can propagate throughout the network. For example, if OpenManage Network Manager discovers a link and it changes the linked port's bandwidth (type ASSOCIATED), it needs to recalculate the TRUNK AGGREGATION for all trunk ports on that device in case the port was an access port and the trunk port bandwidth values need to be updated.

Another example: If an interface's bandwidth value changed, then OpenManage Network Manager adds its parent for INTERFACE AGGREGATION reprocessing in case it has a parent using that calculation type that now needs to be updated.

OpenManage Network Manager uses a strict priority to determine which calculation method to use if multiple are applicable: CONFIGURED > TRUNK AGGREGATION > INTERFACE AGGREGATION > ASSOCIATED > UNCONFIGURED. This means that if a port has a direct QoS configuration against it, it doesn't matter if it also has child interfaces or links. OpenManage Network Manager uses the QoS configuration's value. Likewise, if OpenManage Network Manager calculates a port's bandwidth using INTERFACE AGGREGATION and it has a link, the link does not matter for the purpose of bandwidth calculation since ASSOCIATED is lower priority.

Scheduling Refresh Monitor Targets

Because monitors can address targets that are members of dynamic groups, refreshing these ensures that group memberships are up-to-date. To do this, you can create or alter the schedule for Monitor Target Refresh (in most packages, such a scheduled item appears by default). When executed, this updates monitors with groups as targets based on current memberships. This removes targets no longer members of a monitored group and adds new group members. A seeded schedule refreshes these every six hours, by default.

Refresh Monitor manually by right-clicking in the Resource Monitors table.

Refresh Monitor Targets for Newly Discovered Devices

If you discover a new device that is part of a monitored dynamic group, it may take some time before monitoring includes that device. To provide immediate monitoring, as soon as discovery finds the device, add the *Refresh Monitor* action to the discovery profile. See *Actions on page 61* for more about that Discovery Profile capability.

To make sure this refresh occurs, do *not* override the following in `redcell.properties` (This section defines the actions executed when no default discovery profile exists):

```
#This shows the default order of Task Activities within Resource Discovery
   Options
#The TaskDefOid will be used for identification and true/false will
   determine if they are
#on by default
#format: <TaskDefOid>&&true,<TaskDefOid2>&&false,<TaskDefOid3>&&true
redcell.discovery.taskactivity.order=Resync&&true,\
DataCollectionForGroupOfDevices&&false,\
Discover_Links_for_a_Group_of_Devices&&false,\
Scheduled_Resync&&false,\
Refresh_Monitor_Targets&&true
```

Topological Correlation

A device can appear unresponsive in monitors if devices through which OpenManage Network Manager must access it are down, even though it may be active independently of the condition of its access. Topological correlation take this into account, and produces fewer false MonitorTargetDown events because OpenManage Network Manager attempts to communicate with adjacent devices to the first device in the network topology. OpenManage Network Manager calculates adjacency according link configuration. If adjacent devices are unreachable, then OpenManage Network Manager does not generate a MonitorTargetDown event because this first device is simply unreachable from OpenManage Network Manager at the moment.

Updating Polling Subscriptions

Polling subscriptions on the mediation agent process can get out of sync with the application server process. When the application server and mediation agent start running, whichever one comes online last triggers application server sending the polling subscription and target information to the mediation server. Enabling or disabling performance monitors also sends this information from the application server to the mediation server.

Any time data goes from one machine to another, temporary connectivity issues can arise, along with potential for data loss, so OpenManage Network Manager accommodates this possibility too. If a server is running for a long time (weeks) and the performance monitors have been frequently enabled and disabled, some targets may not be polled because the appserver/medserver information has become out of sync. It's possible, but less likely, that polling and target information could be out of sync even on standalone systems, where the application server also serves as a mediation agent. This is why the following feature is also available on standalone systems.

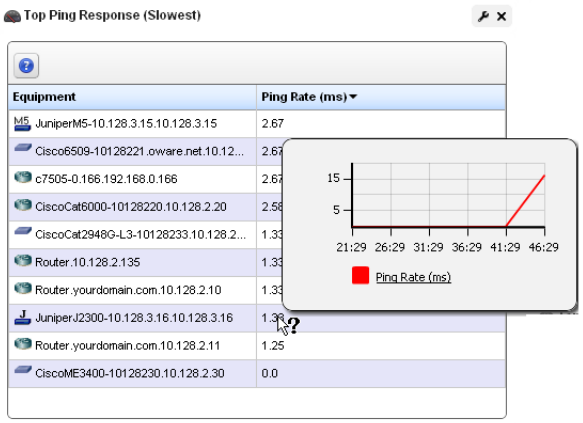
You can schedule periodic resyncs of polling subscription and target information. The scheduled item that runs this process is disabled by default, but if enabled it typically runs every 30 minutes. You can also enable this item and schedule it more or less often than every 30 minutes.

If you enable this scheduled item, or run it a single time manually, then it ensures the mediation agent has all of information it needs for polling. This includes the polling subscription information associated with each active performance monitor and all active targets associated with each active monitor.

Top N [Assets]

This was moved and reworked in the UI description, Appendix A, Performance Page

OpenManage Network Manager uses seeded, default Active Performance Monitors (APM) to display performance data in several categories. These Top N portlets display the summary results of device monitoring, for example, Top Ping Response (Slowest) displays the devices slowest to respond to ping.



Devices appear, ranked by the monitored parameter. Hover the cursor over the Ping Rate column, and a row's a popup graph of recent activity over time appears.

If you right-click a monitored item, you can select from menu items like those that appear in the portlet described in Managed Resources on page 454.

For some portlets (for example Top CPU / Disk / Memory Utilization, Top Interface Bandwidth / Errors), the right-click Performance menu items include Key Metrics. The menu can include *Performance* which displays Dashboard Views related to the selected monitor.

For some packages, these can also include IP SLA statistics like the following: Top Bandwidth Received / Transmitted, Top CPU / Disk Utilization, Top Ingress / Egress Packet Loss, Top Jitter, and Top RT Delay. To see all available *Top* portlets, click *Add* > *Applications* and look below *Top N* on the subsequent panel.

Top RT Delay maps to the AvgRTDelay inventory metric. When no metric for Average RT Delay exists in the MIB, OpenManage Network Manager calculates it the average RT Delay using two mib attributes: RTTSum (the total time taken for all round trips) and NumOfRTT (the number of round trips taken). The calculation of AvgRTT is the value of RTTSum divided by the value of NumOfRTT. OpenManage Network Manager maps this attribute to the AvgRTDelay inventory metric.

NOTICE

An alternative way to provide this kind of performance information is to use Traffic Flow Analyzer. For systems generating large amounts of information that strain the limits of processing capacity, see Best Practices: Performance Tuning Traffic Flow Analysis on page 240 as a possible solution.

Calculations within Top N Portlets

The following lists potentially available Top N portlets. Only those with monitored parameters display data. The data comes from monitor data using the monitor inventory mappings specified in each monitor.

The tooltip graph shows the values for the attribute over the last 30 minutes. The Errors and Discards attributes are counter values that show the change in value since the previous polling cycle. The other attributes are gauges which display a rate or percentage. The value displayed for each entry is the average over the last 30 minutes for the gauge attributes and the sum of values over the last 30 minutes for counter attributes.

These top assets portlets are available from the Performance Summary page or can be added using the Add > Application menu option as needed.

The following portlets display data based on equipment targets:

Top CPU Utilization — Percentage of CPU used. Located on the Performance Summary page by default.

Top Disk Utilization — Most disk use

Top Memory Utilization — Memory use. Located on the Performance Summary page by default.

Top Ping Response (Slowest) — Slowest ping response. Located on the Performance Summary page by default.

The following portlets display data based on port or interface targets:

Top Interface Bandwidth — Most interface bandwith use. Located on the Performance Summary page by default.

Top Interface Errors — Most interface errors. Located on the Performance Summary page by default.

Top Input Discards / Errors — Most input discards / errors. The tooltip/graph that appears when you hover your cursor over a row in these portlets shows the change in discards or errors, then Redecll adds changes to the base value and that sum appears within the table.

The Top Input Errors portlet is located on the Performance Summary page by default.

Top Output Discards / Errors — Largest number of output discards / errors.

The Top Output Errors portlet is located on the Performance Summary page by default.

Top Bandwidth Received / Transmitted — Displays percentage of bandwidth use received or transmitted.

Top Bandwidth Received (bps) / Transmitted (bps) — Displays bandwidth use in bytes per second. Located on the Performance Summary page by default.

The following portlets display data based on SLA or VRF targets:

Top Egress / Ingress Packet Loss — Most egress / ingress packets lost. Located on the Performance Summary page by default.

Top Jitter — Highest jitter rates

Top MOS — Highest MOS (a network performance measurement).

Top Packet Loss — Greatest packet loss. Located on the Performance Summary page by default.

Top RT Delay — Longest round trip (RT) ping delay

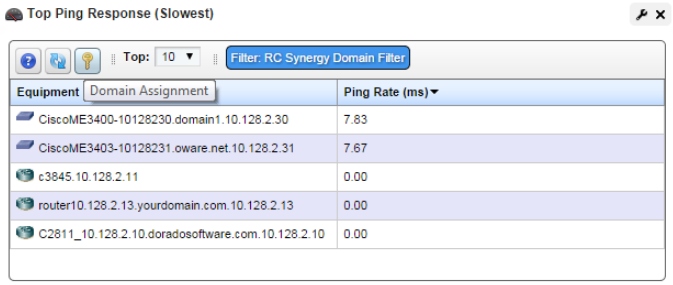
The following portlets are not monitor based

Top Problem Nodes — Devices with the highest alarm state

Top Configuration Backups — The most recent backups

Displaying Tenant Domains in Top N Portlets

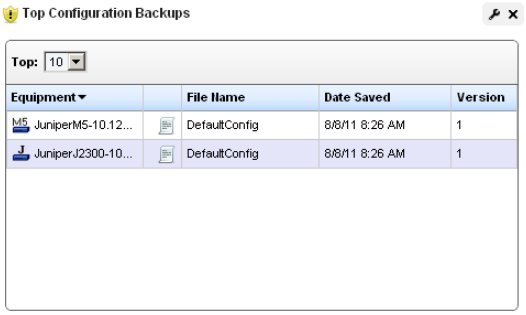
If you have implemented a multitenant (MSP) system, but want the master domain to display Top N for just a tenant domain, the key icon in the portlet's toolbar lets you select different sub-domains.



The filter label in the toolbar displays which domain has been selected. Once you filter a Top N portlet this way, it displays results only for equipment authorized for the selected domain.

Top Configuration Backups

This panel lists the most recent configurations backed up from devices. The pick list in the upper



right corner lets you select not just the top 10 such backups, but the top 5, 10, 15, 20, and 25.

Right-clicking a backup offers the same options as the portlet described in Configuration Files Portlet on page 579.

Dashboard Views

The Dashboard Views portlet lets you assemble several monitors into a single display, or dashboard.



You can create and display dashboards by right-clicking items in the Managed Resources portlet, selecting *Show Performance*, or by selecting *New* in the *Dashboard Views* portlet.

Right-click the listed dashboards, and a menu appears that lets you *Rename*, *Delete*, *Copy*, *Edit*, create a *New* simple or custom dashboard, or *Launch* a Dashboard View (either *Maximize*—a larger view—or as a *Popup*). You can also import/export views and share views with other users on your system. See Dashboard Editor on page 227 for information about creating or modifying dashboards. For an explanation of *Convert*, see *Convert Simple Dashboards to Custom Dashboards* on page 232.

The Performance Dashboard on page 226 and Dashboard Editor on page 227 describe configuring simple dashboards. See the How to: Create a Custom Dashboard View on page 228 section for a description of custom dashboard view creation.

You can also Convert Simple Dashboards to Custom Dashboards, as described below. When you *Edit* a view, Dashboard Editor appears. It lets you select which monitors appear in the dashboard, the monitored entities, and attributes.

The expanded portlet offers similar capabilities.To make a monitor appear on a page, use the portlet described in Performance Dashboard on page 226.

When you create dashboards, data rollup is part of what the display shows. If, for example, the monitor displays the results from a boolean (0 or 1 output), rollup may average values for a duration, and values less than one will appear in the graph.

△ CAUTION:

Revisions like deleting container views from a page require a page refresh before the dashboard works correctly. Some packages contain a *System* dashboard that may not let you select monitors.

Launch a Dashboard View

Launching a view lets you view the monitors active for a Dashboard view.



Some packages display a *Network Dashboard* by default. If the Network Dashboard portlet is blank, you can create a new one. Click the *select new* text in the upper right corner of the portlet to select an alternative, already configured view from those in Dashboard Views portlet. Click the *edit* button in that same corner to alter the configuration of any existing dashboard. See Dashboard Editor on page 227 for more about altering views.

You can configure Dashboards appear by configuring them in the Dashboard Views portlet, or by selecting a device or devices from the Managed Resources portlet, right-clicking and choosing *Show Performance*. To select more than one device, use the expanded Managed Resources portlet.

The first time you create a default template dashboard for a single device, OpenManage Network Manager saves it in the Dashboard Views manager. Invoking *Show Performance* for that device subsequently displays its default view.

The icons in the dashboard's upper right corner let you edit *Dashboard Properties* with the Dashboard Editor, or *Save* the dashboard with the other icon.

NOTICE

No need to reload the browser to update a dashboard; it reloads data every 30 seconds by default, with less overhead.

Displaying Values

Hovering the cursor over the individual points displays the charted attribute value(s) as popup tooltips. If a graph has multiple lines, the data points for different lines are charted at different times (OpenManage Network Manager distributes polling to balance the load on its mediation

service). Hover the cursor over the time when a line's data point appears, and that line's value appears as a tooltip. It may seem a device reporting the same value as others is not graphed properly, but mousing over the graph displays the value.

The legend of devices and/or attributes that appear in each graph also provides interactive features. Hover your cursor over a device or attribute color in the legend and only that device or attribute appears onscreen. By default all such legend color squares contain checks. Uncheck the ones you do not want to see. The legend can appear consolidated or for each chart, as is appropriate to the distribution of charted devices and attributes.

If no data is available for an attribute in a dashboard, no panel appears for that data.

Changing Dashboard Time / Date Format

Control panel's Redcell > Application Settings screen has a *Performance Chart Settings* panel where you can set the *Day Format* and *Minute Format* so dashboards display time (the x axis) in a meaningful way. If you want european date formats (day/month/year rather than month/day/year), this is available if the language / location settings of the operating system on the computer running OpenManage Network Manager makes it available.

In Control Panel's *Performance Chart Settings* panel, you can also enable Threshold display in dashboards and elect to *Restrict Y-Axis Range to data range* with checkboxes.

How To:

Create a Simple Dashboard View

Follow these steps to create a simple dashboard view. See How to: Create a Custom Dashboard View on page 228 for more complex monitor creation.

1. In the Dashboard Views portlet, right click to select *New* > *Simple Dashboard*.
2. Select a name (for example SNMP Interface, to display the monitor configured in How to:Create an SNMP Interface Monitor on page 186).
3. Click *Add Entity* in the Entities panel.
4. In the filter that appears, select the type: Interface.
5. Filter for the IP address of the entity monitored in the previous SNMP interface monitor creation, select it and click *Add Selection* and *Done*.
6. Select the ifInErrors attribute, and click the right arrow in the Dashboard View Attributes panel.
7. Click *Save*. The dashboard view you have configured should appear in the portlet.
8. To launch it, right-click and either *Launch (Popup)* or *Launch (Maximize)*
9. If you want to convert this simple dashboard to a custom dashboard so you can alter it further, right-click and click *Convert*.
10. Notice that you can also change the time/date format as described in Changing Dashboard Time / Date Format above.

NOTE:

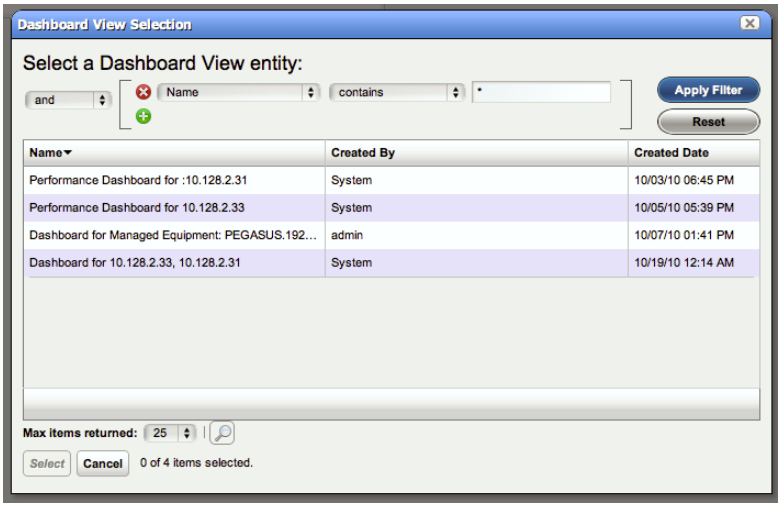
To improve performance, SNMP Interface Monitor does not retain polled data by default. You cannot use historical attribute data in a dashboard without this retention.

Performance Dashboard

This portlet lets you install and configure Dashboard Views as permanent displays rather than portlets. When you initially install this portlet, it appears empty. The message "No Dashboard View has been set:" appears with a *Select* button. Click that button to open the Dashboard View Selection screen.

Dashboard View Selection

This screen displays any existing dashboards so you can select one for the Performance Dashboard you want to appear on a page in OpenManage Network Manager.



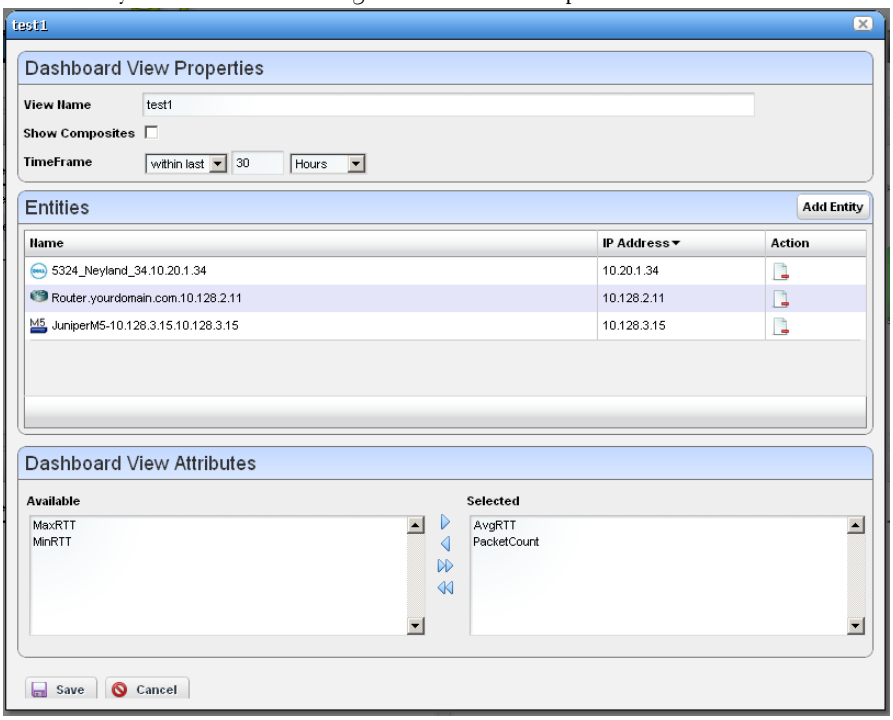
Use the filter at the top of this selector to limit the listed dashboards from which you can select. See Dashboard Views on page 223 for more about creating and configuring the views from which you select.

NOTICE

If you delete the Network Status Dashboard can put it back by adding the Performance Dashboard portlet to the desired page, then select the desired Dashboard View you would like to display as your Network Dashboard.

Dashboard Editor

When you *Edit* a dashboard by right-clicking a resource from the Managed Resources portlet and selecting *Show Performance*, or create (select *New*) a dashboard from the Dashboard Views portlet, an editor appears that lets you select and rearrange the monitor components of the dashboard.



This screen has the following fields:

View Name—The identifier for the dashboard. The default is "Performance dashboard for [IP address]," but you can edit this. This is what appears in the Dashboard Views list.

Show Composites—Show attributes that are constructed from other attributes. Composites attributes are special attributes that consist of the attribute name and the instance name. For example: CPU Utilization:cpu1. Some KPI metrics are composite. If you use SNMP Table monitor, then pretty much all values retrieved are composite.

TimeFrame—Use the selectors to configure the time frame for the performance measurement displayed.

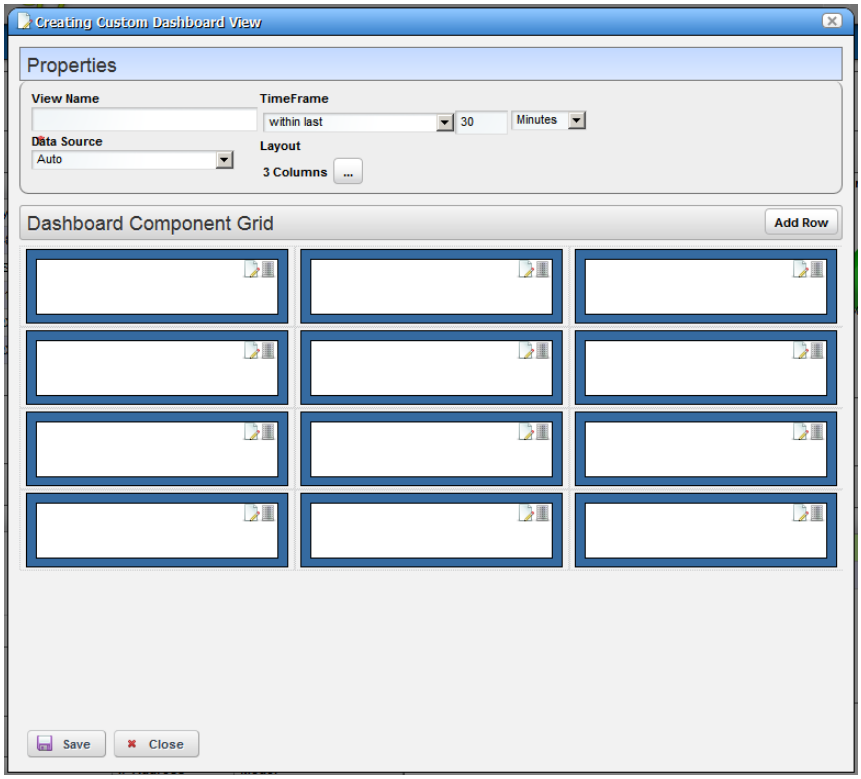
Entities—Select the equipment you want to monitor. When you right-click to *Show Performance* with resource(s) selected, those resources appear in this list.

Dashboard View Attributes—Click the arrows between *Available* and *Selected* panels to select monitors for the dashboard. The Available Attributes list shows all the available attributes for that device based on its monitor affiliations. If you select none, a chart appears for each attribute that has data. This is the default. If the user moves some attributes to the *Selected* list then only charts for those attributes appear.

How To:
Create a Custom Dashboard View

The following steps create a custom dashboard view:

1 In the Dashboard Views portlet, select the *New Custom Dashboard* command. An empty default view with twelve components appears.



The Properties panel contains the following controls:

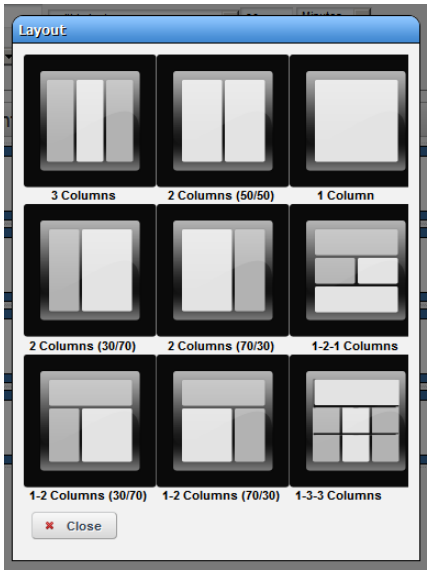
View Name—The name of the dashboard view (Required)

Time Frame—The period over which to display the data. May be either relative (like *last 30 minutes*) or absolute (between specific dates and times). The specified frame applies to all charts in the dashboard.

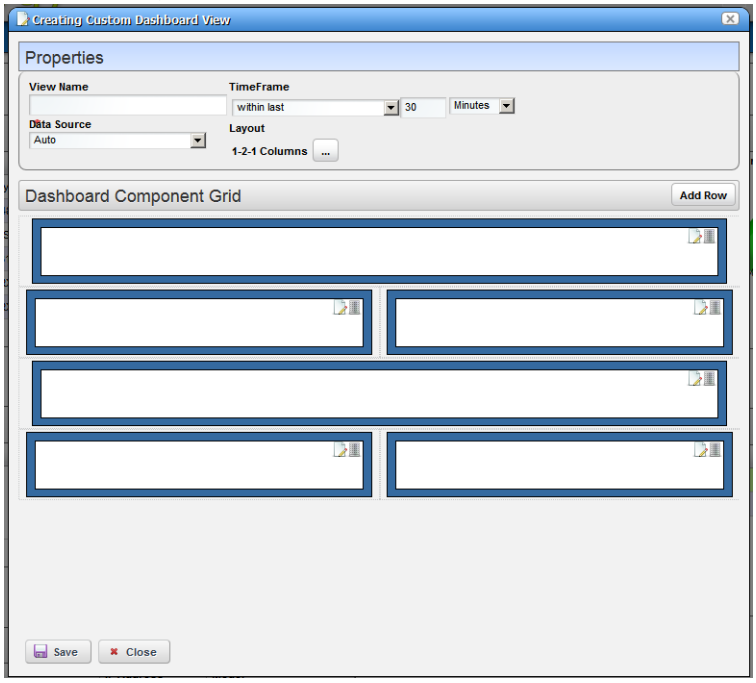
Data Source—Source for the data. *Current* displays current (raw) data. *Hourly* displays rolled up hourly data. *Daily* displays rolled up daily data. *Auto* (default) determines which data source to use based on the selected time frame.

Layout—Select the desired layout style used to display the dashboard components.

2 To select a layout style, click on the ... button next to the current layout. The layout chooser appears.



3 Click on the desired layout or click *Close* to keep the current layout. The components displayed to reflect the selected new layout.



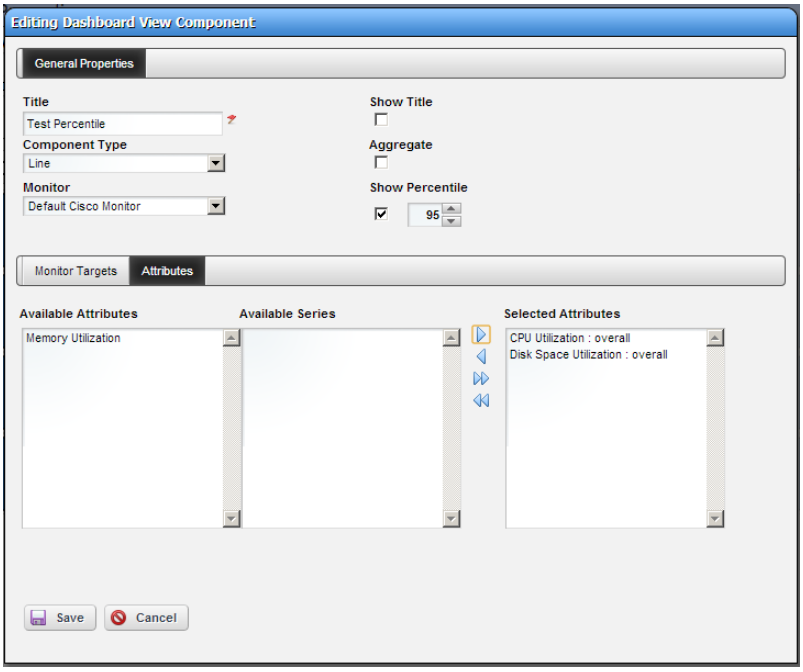
If no dashboard components have been configured yet a default configuration appears with three or four rows depending on the dashboard style. If the dashboard components have been configured it will create at least enough rows to display all the configured dashboard components. Add more rows by clicking on the *Add Row* button. An individual dashboard component can be deleted by clicking on the delete button on the component.

Moving Dashboard Components

4 To move a dashboard component to another location, click and drag it over another component. When you release the mouse, the components exchange places.

Configuring Dashboard Components

5 To configure a dashboard component, click the *Edit* button in the upper right corner of the component. The component editor appears.



The following properties appear in the General Properties section:

Title—Title of this component (required).

NOTICE

Dashboards with a single attribute do not display units, so including them in the title may be informative.

Show Title—Check to display this title above the chart for this component. This overrides the default title that is shown for some charts.

Aggregate—Aggregate the monitored attributes. The aggregate is a sum of all the values for all the entities in the current context.

Show Percentile—Check to enable showing a percentile line for displayed data. Configure the percentile in the field and spinner combination that appears after you check to enable it.

A blue line appears on the dashboard at the selected percentile of the displayed data. If you selected 95%, then of 100 data points, five would be above the line, and 95 below it (so the calculation is more like median than mean). A tooltip for this line displays the calculated value and the selected percentile.

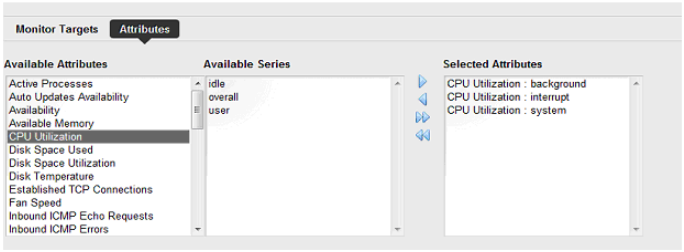
This only supports one line per chart for percentile. If more than one line is on the chart, this computes the percentile based on the first line.

Component Type—Combo Box which specifies what type of component to create. These include the following chart types, *Line*, *Dial*, *Bar*, *Top Talkers* (a line chart showing the top [or bottom] n components for a specific attribute on a specific monitor) *Top Subcomponents* (a line chart showing the top [or bottom] n subcomponents belonging to a specific device for a specific attribute. See

Other controls appear depending on the component type selected. These components also have a *Monitor* control, a pick list where you can select from which monitor the charted data originates. See Dial Chart Properties, Top Talkers Properties and Top Subcomponents Properties below for specifics about those.

The line and bar components have two tabs under the general properties section: *Monitor Targets* and *Attributes*. The Monitor Targets section lets you select the devices that are sources of data. You can select any device or attribute in the previously selected monitor. Click the *Add* button displays the monitor target selector.

6 The Attributes tab selects the attribute(s) that appear in the chart. If an attribute is a composite, then its series appears in the Available Series listbox.



Select the desired series and click the right arrow to move them to the Selected Attributes listbox.

If the attribute is not a composite, then nothing appears in the Available Series listbox. Here, click the right arrow to move the attribute to the *Selected Attributes* listbox.

You can also elect to *Show Title*, *Aggregate* (show composite attributes), or *Show Percentile* (display a line at the 95th percentile on the graph) by checking the checkboxes.

Dial Chart Properties

Dial charts have the following additional properties

Monitor—Select which monitor the charted data comes from in the pick list.

Attribute—The attribute to get data for. Note that for aggregate data, each attribute has a minimum (min), maximum (max), and base attribute . If the period is set to Detail, then the aggregate values will always be zero.

Min / Max Value—The minimum / maximum value on the dial.

Entity—The monitor target to get the data for. Clicking on the + button brings up the entity selector.

Top Talkers Properties

Top Talkers components have the following properties.

Monitor—Select which monitor the charted data comes from in the pick list.

Attribute—The attribute to get data for.

NOTE:

For aggregate data, each attribute has a minimum (min), maximum (max), and base attribute . If the period is set to Detail, then the aggregate values will always be zero.

Max # of Entities—The number of entities to display

Order—Select either *Ascending* (Bottom n), or *Descending* (Top n).

Top Subcomponents Properties

Top Subcomponents components have the following properties.

Entity—The parent entity for the found subcomponents. Clicking on the + button brings up the entity selector.

Attribute—The attribute to get data for.

Max # of Entities—The number of entities to display

Order—Select either *Ascending* (Bottom n), or *Descending* (Top n).

Convert Simple Dashboards to Custom Dashboards

To convert a simple dashboard to a custom dashboard use the *Convert* command on the *Dashboard Views* menu. You cannot convert custom dashboards to simple dashboards.



How To:

View Historical Dashboard Data:

1. Click on the clock icon in the dashboard header.
2. Change the timeframe to the period on the day for which you want to view data.
3. Click on the green checkmark.
4. The data appears for the selected time frame.

On simple dashboards the type of data (raw, hourly, daily) depends on the timeframe selected. For less than three hours, raw data appears. For three hours to less than three days, hourly data appears. For three days or more daily data appears.

Do not forget you may need to change the data retention policy. You may not see raw data if you are viewing a timeframe from two days ago because the default retention policy only keeps raw data for one day.

Show Performance Templates

By default, the Show Performance command displays data for the first twelve attributes it finds. You can control which attributes appear when you select Show Performance by creating a performance template. A performance template lets you set dashboard parameters and associate them to one or more device models. Then, when you execute Show Performance on a device of that type, those dashboard parameters display the dashboard for that device.

How To:

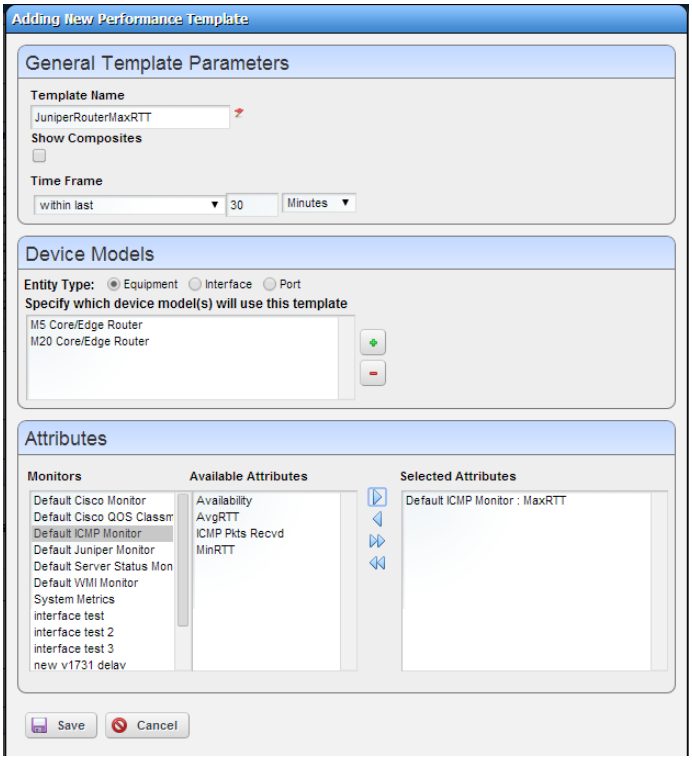
Create A Performance Template

To create a performance template, follow these steps:

1 Right click in the Dashboard Views portlet and click on the *Performance Templates* menu item.

2 The Performance Templates manager appears.

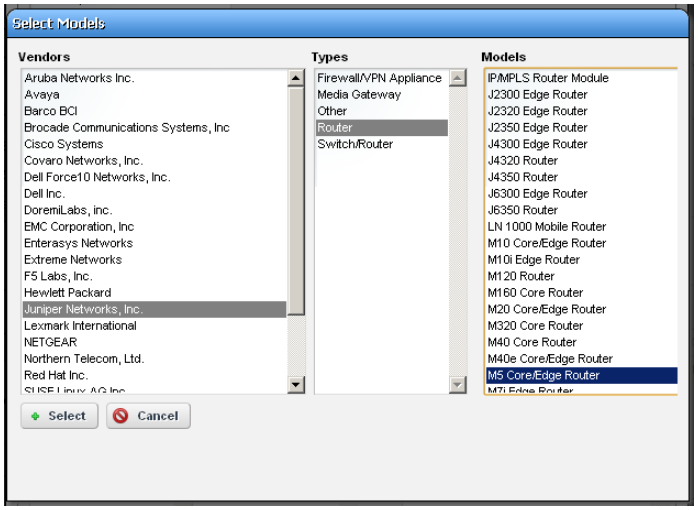
3 To create a new performance template, click on the Add button. The Performance Template Editor appears.



For this example, we have selected *Entity Type: Equipment* with the radio buttons below *Device Models*. See *Dashboard Templates for Interface and Port Equipment* on page 235

4 Name your template. The Show Composites and Time Frame fields are the same as in the dashboard (see Dashboard Editor on page 227).

5 To specify which device model(s) this template will apply to, click on the + button in the Device Models panel. The model selector appears.

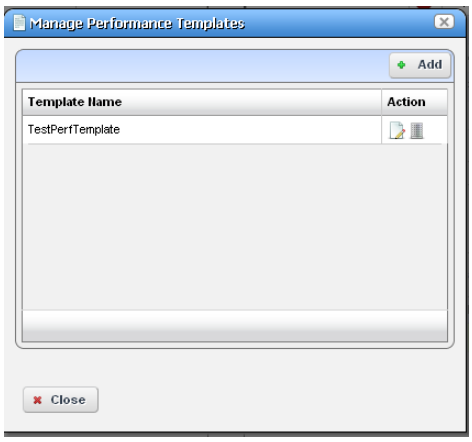


Select multiple devices by clicking + repeatedly, selecting a single device each time. You can also make several templates for each device. See Multiple Performance Templates on page 235 for the way that works.

6 Click on a vendor to see the device types for that vendor. Then click on a device type to see the models available for that vendor and device type. Select the model you want and click on the select button.

7 To select the attributes that you want to appear by default in a performance dashboard for the selected device, click on a monitor to see the attributes available for that monitor. Click on the right arrow button to move the selected attributes from *Available* to *Selected*. Those are the attributes that will appear by default in dashboards for the selected device.

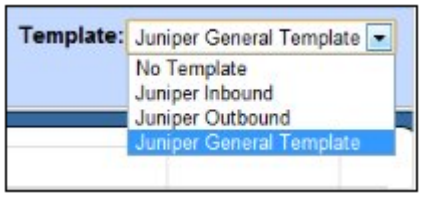
8 When you have selected all the parameters you want, click *Save*. It then appears in the template list.



To edit or delete your template, use the buttons in the action column of the table.

Now when you click on show performance, OpenManage Network Manager checks whether a template for that device type exists. If one exists, then that template guides what appears in the performance view for the device.

Multiple Performance Templates

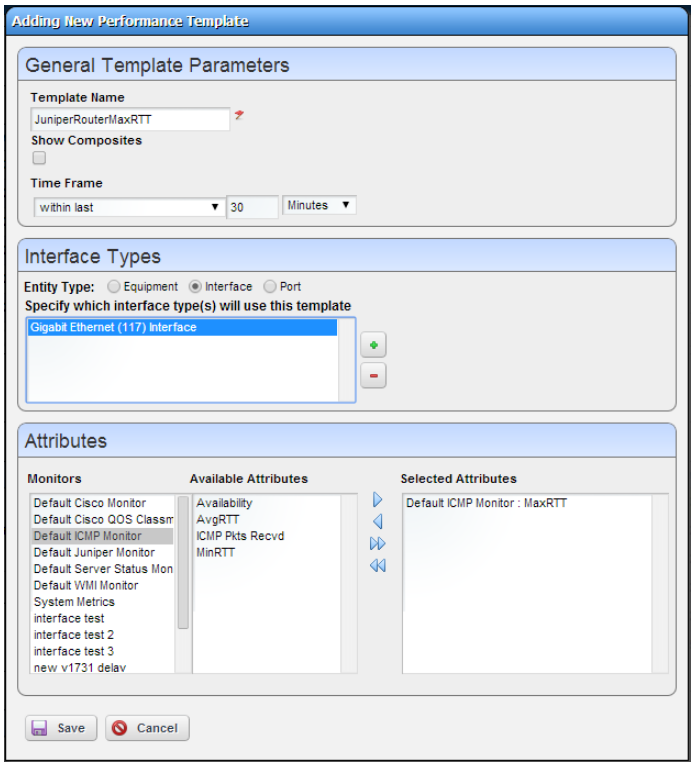


The template name appears in the upper right corner of dashboards that appear when you select Show Performance.

If other templates for that device type exist they also appear in a template pick list in the upper right corner. You can pick another template to display its attribute selection. The *No Template* selection displays the default dozen attributes that would appear if you selected Show Performance without a template defined for the device.

Dashboard Templates for Interface and Port Equipment

Dashboard template types include Interface and Port templates. When configuring a dashboard template in the editor (see How to: Create A Performance Template on page 233), select the *Interface* or *Port* radio button in the middle panel of the editor, then add the appropriate port or interface in that same middle panel.



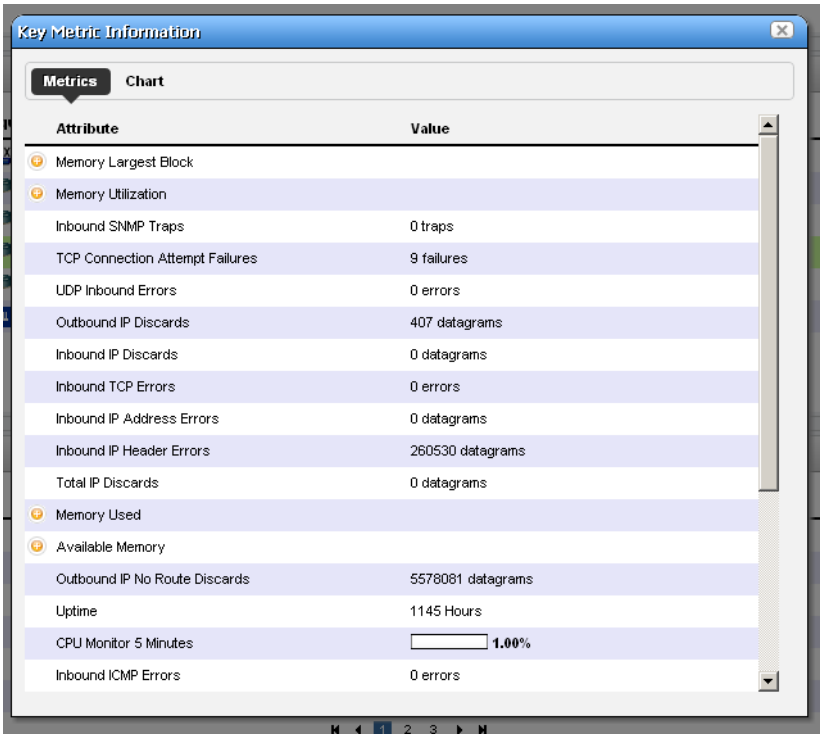
After selecting the port or interface types for the template, you can select the Attributes to monitor as you would for other equipment.

Key Metric Editor

When you select *Performance* > *Show Key Metrics*, this editor appears for devices that have such metrics. It displays the available Metrics, and a Chart panel where you can configure their display.

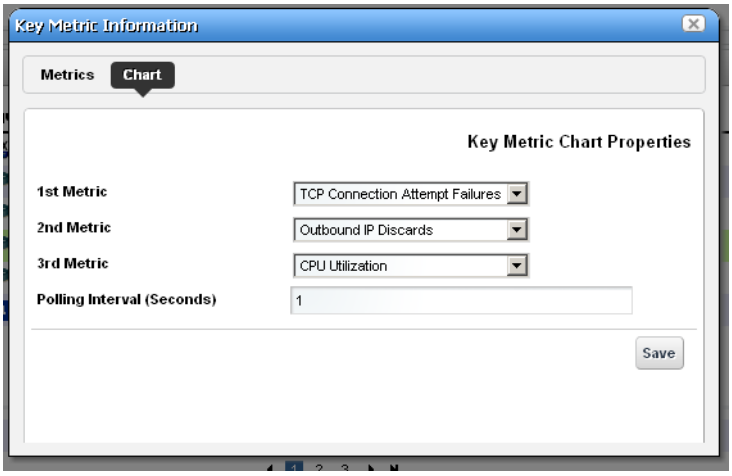
Metrics

This panel's display depends on the selected device.

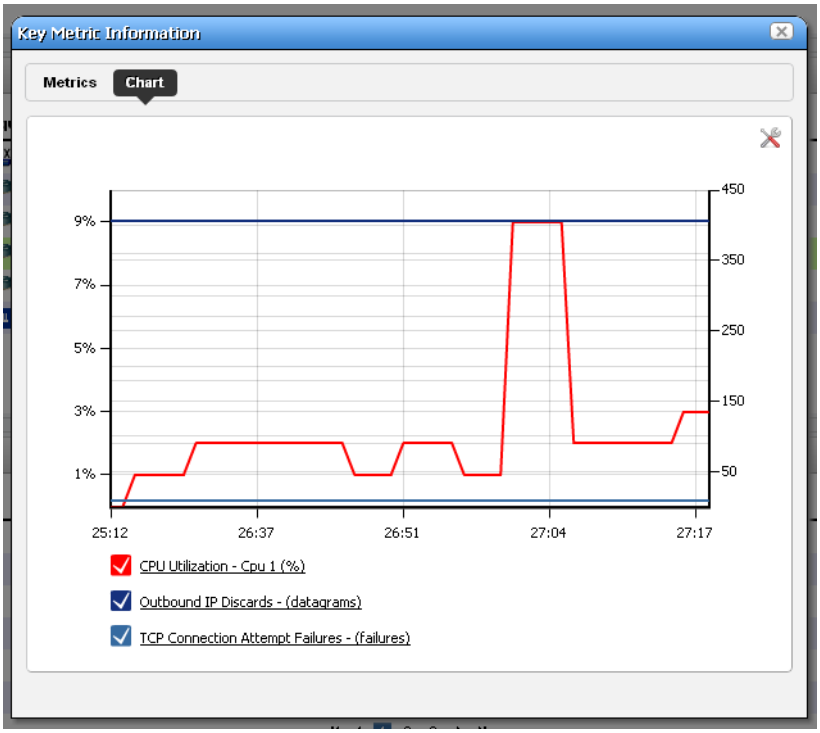


Chart

Click *Chart* to first select up to three metrics you want to graph, and the polling interval for the graph.



Then click *Save*, and the graph appears.



Click the screwdriver / wrench icon in the upper right corner to return to the chart configuration screen.

9

Traffic Flow Analyzer

OpenManage Network Manager's Traffic Flow Analyzer listens on UDP ports for packets in the NetFlow and sFlow family of protocols (this includes NetFlow implementations such as JFlow, NetStream, etc). A flow is a unidirectional stream of packets between two network nodes. The following key parameters appear in flows:

Source IP address

Destination IP address

Source port number

Destination port number

Layer 3 protocol type

ToS byte (Type of Service)

Input logical interface

Using that data, Traffic Flow Analyzer can help you visualize network traffic, troubleshoot and anticipate bottlenecks.

NOTE:

Typical packages come with a default limit to the number of monitored devices. Upgrade your license if you want to exceed the package limit. Because of the performance demands they make, Traffic Flow exporters are licensed separately from the managed resource license count, so a license to manage 50 devices does not necessarily let you have 50 Traffic flow exporters.

Traffic Flow Analyzer support in OpenManage Network Manager collects and process flows with source and destination IP address. Switches or devices that only support L2 flow payloads with MAC address as the source and destination payload are not currently supported. Example: Juniper EX devices.

Supported versions include sFlow v5, and NetFlow v5 and v9, but not previous versions (for example, v2).

Parse errors can appear in the application server log for some flow data.

```
Parse error: Unable to process non IP type flow. Type: <Number>
```

`<Number>` represents an sFlow packet type. This application only parses data of type `IP`. When OpenManage Network Manager receives non-IP packets, it drops packets and this error appears.

OpenManage Network Manager typically limits the number of exporters available for your system through licensing. Review your Traffic Flow Analyzer license setting in the license viewer under Product Licenses tab, the license detail section (MaxExporterCount=n, where "n" is the number

of exporters licensed.) After reviewing recommendations for performance tuning and hardware sizing in this document, you can request a license allowing more exporters from your sales representative.

Best Practices: Performance Tuning Traffic Flow Analysis

Most OpenManage Network Manager packages limit Traffic Flow exporters through licensing, however be aware that even small numbers of traffic flow exporters may overwhelm hardware resources. For example even if you monitor as few as one to five nodes export data with a very high sampling rate and have high traffic volumes, the amount of data that needs to be inserted into the database may quickly exceed the insertion rate capacity of a single 7200 RPM disc. The performance limitation imposed by the demands of Traffic Flow Analysis is one motivation to tailor monitored flows to fit within the limits of your hardware.

You may also need to edit or fine-tune several default configurations to accommodate the volume of traffic flow data exported from the managed devices and to manage the resources (processing power, total memory) available to OpenManage Network Manager.

XML and properties files in `/owareapps/trafficanalyzer/server/conf/` contain these configuration settings. The `ta-service.xml` configures standalone environments, `ta-med-service.xml` configures distributed environments, and for additional configuration, edit `ta.properties`. Any edits requires an application server and/or mediation server restart to take effect.

NOTE:

Best practice: Contact Dell EMC support for assistance before editing these files.

In `ta-service.xml` and `ta-med-service.xml`, you can edit the entry for the NetFlowListenerMBean, like the following:

```
<mbean code="com.dorado.netflow.NetFlowListenerMBean"
    name="oware:service=NetFlowListenerMBean">
<attribute name="ReceiverUDPPort">9996</attribute>  <!-- # NetFlow UDP
    port -->
<attribute name="ReceiverTopNToKeep">0</attribute>  <!-- Number of rows
    per time bucket to keep -->
<attribute name="RecvQueueMaxSize">10000</attribute>  <!-- # unparsed
    packets -->
<attribute name="RecvQueueLowThreshold">80</attribute>  <!-- Low threshold
    for packet queue as pct -->
<attribute name="UnparsedMaxSize">10000</attribute>  <!-- # unparsed v9
    flows entries waiting on template -->
<attribute name="TransportBatchSize">1000</attribute>  <!-- # NetFlow
    values (inserts) and session summaries (updates) -->
<attribute name="TransportBatchTimeout">10000</attribute>  <!--
    milliseconds -->
<attribute name="SpoolQueueMaxSize">10000</attribute>  <!-- # NetFlow
    session results -->
<attribute name="SpoolBatchSize">50</attribute>  <!-- # NetFlow session
    results flushed at a time to disk during overflow -->
<attribute name="SpoolFileBufferSize">131072</attribute>  <!-- # bytes for
    I/O buffer -->
<attribute name="SpoolFileName">@OWARE_USER_ROOT@/owareapps/
    trafficanalyzer/temp/tadata_spool.dat</attribute>
<attribute name="SpoolMaxFileSize">41943040</attribute>  <!-- # bytes for
    disk allocation -->
```

```
<attribute name="EnabledDNSLookup">true</attribute>  <!--#Enabed DNS
    lookup-->
<attribute name="SamplingRate">1</attribute>  <!-- #Sampling Rate-->
<depends>oware:service=NotificationProcessingMBean</depends>
<depends>oware:service=HAServiceController</depends>
<depends>oware:service=ClusterPrimaryDesignator</depends>
<depends>jboss.j2ee:jndiName=RuleEngine,service=EJB </depends>
</mbean>
```

CAUTION:

Changes to this file do not persist if you upgrade. Best practice is to save a copy of the file elsewhere, and re-copy it into the correct location after upgrading.

Using "Top N to keep" to deal with high-volume scenarios

Sometimes the volume of traffic flow data collected from the exporters can overwhelm the database. OpenManage Network Manager collects traffic flow packets (sFlow, NetFlow) from the registered exporters and aggregates the data into 1-minute flows differentiated by exporter, protocol, application, and conversation (including sender and receiver for both IP and autonomous systerm). Every minute, these flow records are inserted into the database. The number of distinct flows, differentiated by each of these fields, can sometimes add up to more row inserts than the database can handle in a single minute. In such cases, the only way for the system to function is for it to only insert the conversation-based flows that are the most significant (highest byte totals) and allow for the less significant flows (low byte totals) to be aggregated into a single flow that represents all other conversations.

This can be done through the "Top N to keep" feature. This feature is disabled by default, but if enabled it will reduce the number of inserts to the database per minute while preserving the most significant flows and also while preserving the overall byte and packet totals. What this means is that if you enter a number for "Top N to keep" then you are configuring OpenManage Network Manager to keep that many flows per minute. So this many flows will be inserted into the database as differentiated by exporter (by equipment manager and by subcomponent), protocol, application and conversation (sender and receiver) but any flow above this number will lose their conversation data and will only be differentiated by the other three fields (exporter, protocol, and application). It does this by first ranking all flows by estimated total bytes and then taking the highest N and inserting each of these into the database as they were reported by the device. The rest of the flows are then aggregated into the "Other" category and inserted into the database.

For example flows with estimated total values of 3, 15, 44, 89, 248, 510, 746, 1038, 4313, and 9755 and "Top N to keep" of 5 would find the top 5 to be 510, 746, 1038, 4313, and 9755. These flows would have their sender and receiver data (IP and AS) saved in the DB but the values 3, 15, 44, 89, and 248 would be added together into the "Other" category, but their protocol, application, and exporter data would be preserved. So these smaller flows would only actually be aggregated if they were all for the same exporter, protocol and application.

To enable this feature, add the following like to installed.properties with your chosen value of N to the right of the equals sign and the restart the application server:

NetFlowListenerMBean.ReceiverTopNToKeep=

Using random sampling to deal with high-volume scenarios

If the volume of incoming traffic flow data is beyond what can be processed, you can tune displays to optimize samplingRate. The sampling rate determines processing speed for incoming NetFlow packets (this does not apply to sFlow packets). The sampling rate should be 1 if you want to try to process everything. If the system is unable to keep up, then set this parameter higher, for example:

10, and restart the server. This makes OpenManage Network Manager process only 1 out of every 10 incoming NetFlow packet, at random. The object is to find the lowest value for this attribute that still allows the system to fully process all records that it tries to process.

To enable this feature, add the following like to installed.properties with your chosen value of N to the right of the equals sign and the restart the application server:

NetFlowListenerMBean.SamplingRate=

Advanced Performance Tuning

You might need to add entries to installed.properties to override the following system properties:

NetFlowListenerMBean. SpoolQueueMaxSize—The maximum number of traffic flow records storable in the spool queue during internal processing. Such processing occurs after OpenManage Network Manager receives them from the exporter and before they are saved to the database. OpenManage Network Manager temporarily stores such records in the spool queue if Traffic Flow Analysis receives more traffic flow packets from the exporter than it can process at once. This allows Traffic Flow Analysis process these records later, packets arrive more slowly. If packets consistently arrive at a faster rate than OpenManage Network Manager can process them, the spool queue fills up and Traffic Flow Analysis discards them without processing.

ta.ThreadPoolSize — The default number of threads working to process traffic flow data.

ta.MaxThreadPoolSize — The maximum number of threads working to process traffic flow data.

Traffic Flow Database Advice

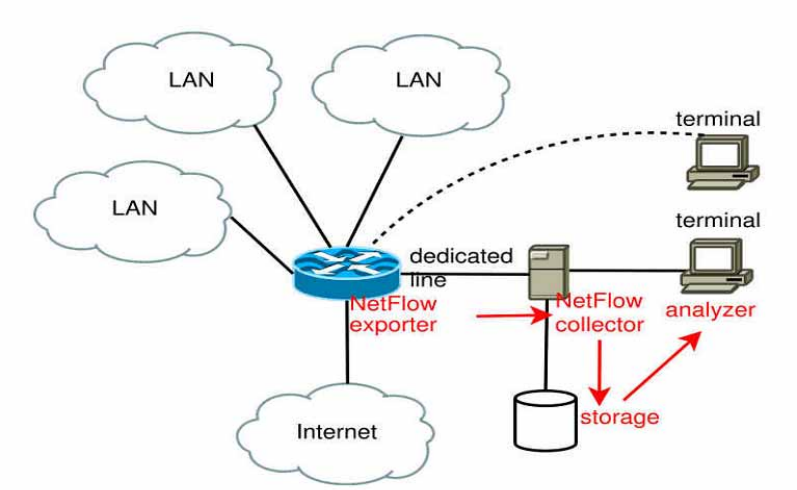
Traffic flow records average 300 bytes. Retention policies determine how long they stay in your database. So 1 minute flows, retained for 48 hours, 50% correlated (Correlation factors indicate the percentage of flows across all one minute buckets being aggregated that correlate based on conversation key data), mean 2.7 million flows per interval. If your retention keeps these 48 hours, then there are 2,880 retained intervals, and 7,776,000,000 potential rows. These rows times the 300 byte record size equal 2,173G in space, and 45,000 inserts per second. Typically, retention is for 1 minute, 10 minute, hourly, daily and weekly intervals, so for an overall picture of database needs, you would need to add all these intervals.

See Best Practices: Performance and Monitors on page 157 for more about calculating database space and hardware and tuning monitored data.

Traffic Flow Limitations

- If you receive no endpoint flow data, the Traffic Flow Analysis form appears empty when you select endpoints. Make sure you are receiving flow data before concluding the device or OpenManage Network Manager is defective.
- The flows received are just samples, and consequently are only as accurate as the polling interval and size of the flows sent. Fewer polling and smaller packets mean less accuracy. For example If you only get 1 packet over the course of a file FTP it will not show the entire file size.

How does Traffic Flow work?



- The NetFlow / sFlow exporting router monitors traffic traversing it
- ...and the router becomes an Exporter of NetFlow / sFlow data.
- It forwards information to the NetFlow / sFlow Collector
- Collector stores, correlates and presents the information about
- Traffic bottlenecks in networks.
- Applications responsible for bandwidth utilization.

Definitions

NetFlow—NetFlow is a traffic profile monitoring technology

jFlow—Juniper's implementation of NetFlow.

sFlow—For Delldevices.

Collector—Application listening on a UDP port for NetFlow / sFlow datagram.

Exporter—Network element that sends the NetFlow / sFlow datagram.

Conversations— IP communications between two network nodes.

Flow—A flow is a unidirectional stream of packets between two network nodes.

NOTE:

Counter sFlows do not appear as Traffic Flows, but essentially duplicate Performance metrics for interfaces. Such Flows monitor how data traverses between *two* endpoints. You can monitor interfaces with Performance monitors. See Performance Monitoring.

Setup

If they are not already set up to emit flow information, set up devices themselves to emit flow data. Consult the manuals for your devices for instructions about how to do this. Make sure your setup does not overwhelm OpenManage Network Manager with information.

Set up OpenManage Network Manager with the following:

Exporter Registration—To register a device, right-click in Resources portlet, after you select the router and choose *Traffic Flow Analyzer > Register*. The system should then be ready to accept flow data from the device.

Router Configuration—You must configure the router to send flow reports to the OpenManage Network Manager server on port 9996 (UDP) for NetFlow (including implementations such as jFlow etc) and 6343 for sFlow by default.

Resolving Autonomous System (AS) Numbers—OpenManage Network Manager provides local resolution of autonomous system numbers (ASN) based on static mapping of AS number registrations. It also supports user overrides to the default mappings. To do this, configure properties you can find in the `\owareapps\trafficanalyzer\lib\ta.properties` file. Remember, best practice is to override properties as described in Overriding Properties on page 71.

Setup Examples

The following sections show example setups for some vendor's devices:

Juniper configuration:

```
configure private
set services flow-monitoring version9 template ipv4-test ipv4-template
set forwarding-options sampling input rate 1
set forwarding-options sampling input run-length 0
set forwarding-options sampling family inet output flow-server
    192.168.52.103 port 9996
set forwarding-options sampling family inet output flow-server
    192.168.52.103 version9 template ipv4-test
set forwarding-options sampling family inet output inline-jflow source-
    address 10.20.1.167
set interfaces ge-0/0/3 unit 0 family inet sampling input
commit
```

Configuring s-flow on Juniper EX series:

For more about this, see:

http://www.juniper.net/techpubs/en_US/junos10.4/topics/example/sflow-configuring-ex-series.html.

```
[edit protocols]
set sflow collector 10.204.32.46
set sflow collector udp-port 5600
set sflow interfaces ge-0/0/0
set sflow polling-interval 20
set sflow sample-rate egress 1000
```

Dell Power connect configuration

```
sflow 1 destination owner Milan notimeout
sflow 1 destination 192.168.0.51
sflow 2 destination owner Terry notimeout
sflow 2 destination 192.168.52.103
interface Te1/0/11
sflow 2 sampling 1024
```

```
sflow 2 polling 256
```

NOTE:

Dell Powerconnect devices allow only one collector per port.

Cisco Example

The following outlines setup for Cisco XR 12000 series and Cisco ASR series routers which require NetFlow v9. The configuration and use of the following maps are the basis of the NetFlow infrastructure:

- Exporter Map
- Sampler Map
- Flow Monitor Map

Exporter Map:

To configure the Exporter map, define the destination (flow collector), the source interface, the port used for exporting, the version of NetFlow, and the timeout rates.

```
router(config)# flow exporter-map SCRUTINIZER-EM
router(config-fem)# destination 10.1.1.5
router(config-fem)# source gi0/0
router(config-fem)# transport udp 2055
router(config-fem)# version v9
router(config-fem)# template data timeout 60
router(config-fem)# options interface-table timeout 60
router(config-fem)# exit
```

Sampler Map:

The Sampler map defines the sample rate, default for the ASR series is 10000, no default for the XR 12000, but recommended sample value is 10000 for optimal performance.

```
router(config)# sampler-map SCRUTINIZER-SM
router(config-sm)# random 1 out-of 10000
router(config)# exit
```

Flow Monitor Map:

The Flow Monitor map defines the cache timeout values and associates the exporter map with this map.

```
router(config)# flow monitor-map SCRUTINIZER-FMM
router(config-fmm)# record ipv4
router(config-fmm)# exporter SCRUTINIZER-EM
router(config-fmm)# cache timeout active 60
router(config-fmm)# cache timeout inactive 15
router(config-fmm)# exit
```

Apply the maps to the interfaces.

Once maps are defined, apply the Flow Monitor and Sampler maps to each active interface:

```
router(config)# interface Gi0/0
router(config-if)# flow ipv4 monitor SCRUTINIZER-FMM sampler SCRUTINIZER-
    SM ingress
router(config-if)# exit
```

For more information on these commands, refer to Cisco's manuals.

How To:

Use Traffic Flow Analyzer

1 Register the device(s) you want to analyze. (As in Exporter Registration). A message confirms registration's success.

NOTICE

You can also display a *Registered* column in the Managed Resources portlet, and click the heading to sort the registered Flow exporters to the top of the display.

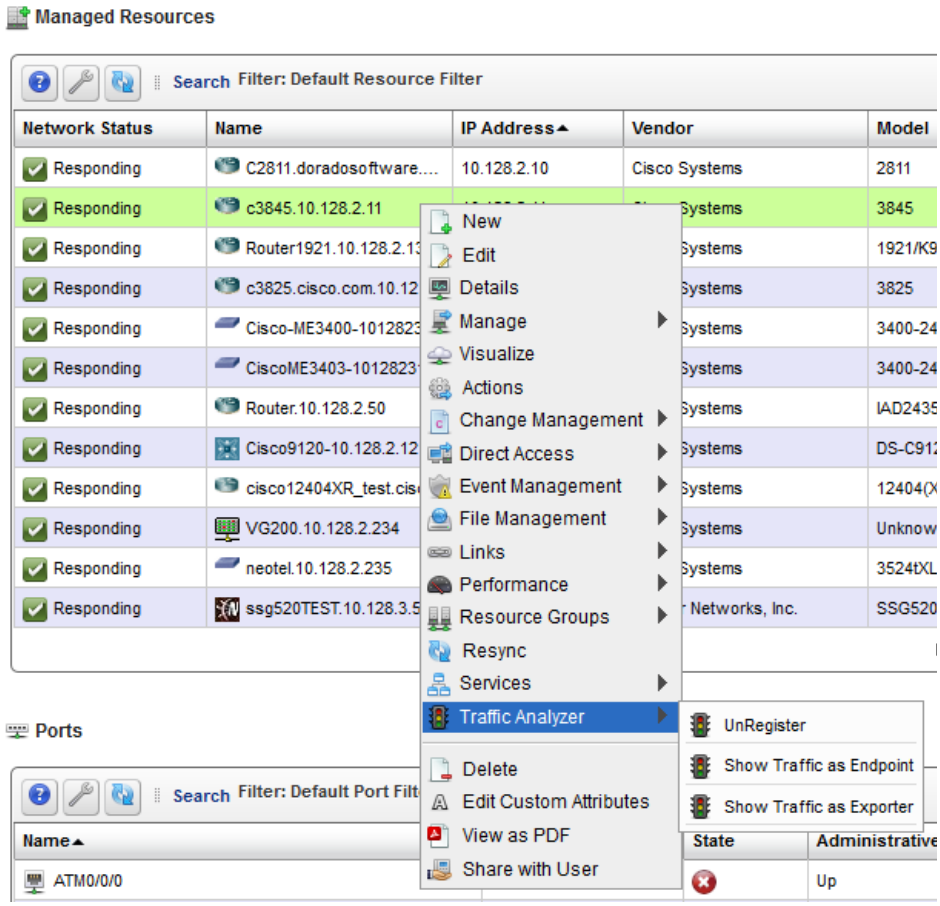
2 Look in the Traffic Flow Portlet for the flows captured.

3 Remember, you can Drill Down to specific data, and Search for specific devices monitored.

For more about Traffic Flow in context of network management, see Traffic Flow Analyzer - Example on page 257.

Exporter Registration

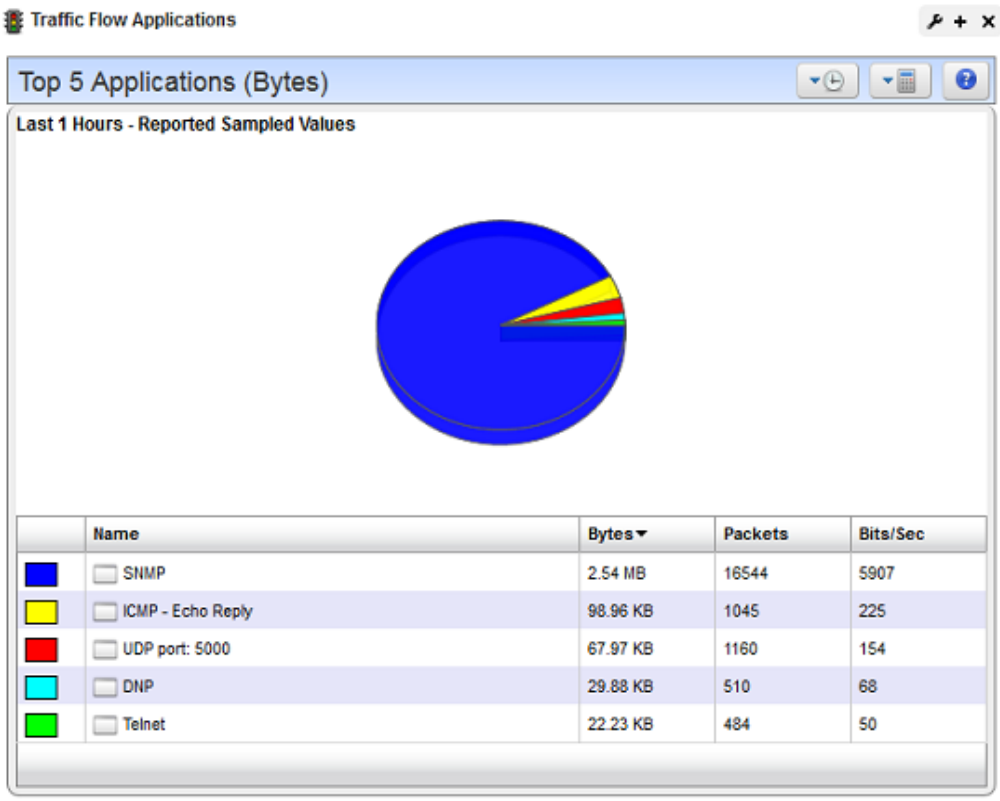
Before you can collect traffic data from a device, you must *Register* it as a traffic flow exporter. If a device is not registered, the *Register* command appears in the menu. If it is registered the *Unregister* command appears. When you successfully register an eligible device, a success message appears; otherwise, a failure message appears, and no registration occurs.



The *Show Traffic* menu options navigate to full-screen views of the expanded Traffic Flow Portlet. Show Traffic as Endpoint is available for all managed devices and cliking this option shows the traffic going through this exporter. Once the expanded Traffic Flow portlet is shown, a pick list of available information types will also be available.

This displays the *Exporters Detail*, *Top 5 Applications*, *Top 5 Autonomous Systems*, *Top 5 Conversations*, *Top 5 Endpoints*, *Top 5 Protocols*, *Top 5 Receivers*, and *Top 5 Senders* related to the device selected before right-clicking. Select a type and click the *Refresh* double arrow to the right of the selector.

The screen that then appears has the features of the Expanded Traffic Flow Portlet described

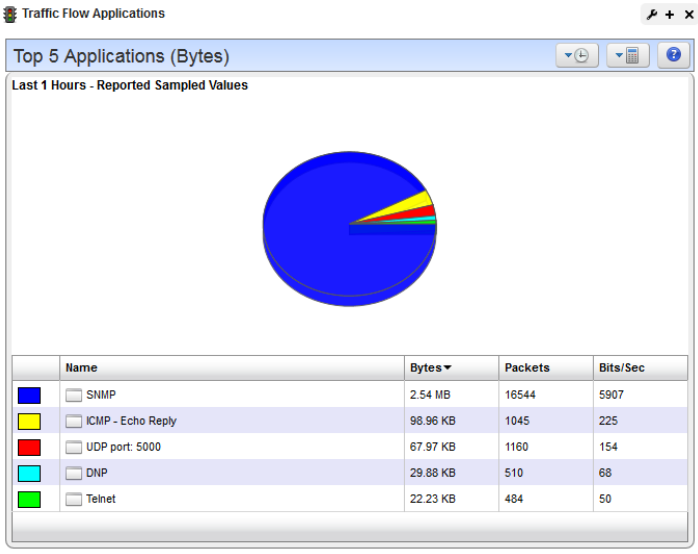


below. See also How to: Use Traffic Flow Analyzer on page 246.

Traffic Flow Portlet

Traffic Flow Analyzer uses several types of portlets, one for each of the types of objects on which it reports. These are Applications, Autonomous Systems, Conversations, Endpoints, Exporters by Equipment Manager, Exporters by Subcomponent, Protocols, Receivers and Senders. Note that Endpoints, Conversations, Receivers, and Senders all have similar data. The way it works is that every flow has a sender and a receiver, and these are both considered endpoints. Also if endpoint A sends a packet that is received by endpoint Z and then Z sends another packet back to A, these packets are both part of the same conversation between A and Z.

When you add one of the traffic flow analyzer portlets to a page, its summary, or minimized form appears. This displays a simple view containing a pie chart and a table showing the summarized collected data over the configured time period. Only the time frame (shown with a clock icon), the mode of calculation (shown with a calculator icon), and the flow direction (ingress, egress, or both) can be changed in this view. These controls appear as dropdown buttons in the upper right corner of the portlet. Most minimized traffic flow portlets are limited to the top entities as measured by total bytes. The minimized Exporters by Equipment Manager portlet is not limited to 5 entries. It supports pagination in the event that there are lots of exporters, so that all the necessary data can be shown.



To see more information about any item within the minimized traffic flow portlet, you can click on the name and this will navigate to the expanded traffic flow portlet, as shown in the context of the selected item. Another way to navigate to the expanded portlet is to click on the + sign in the upper right corner.

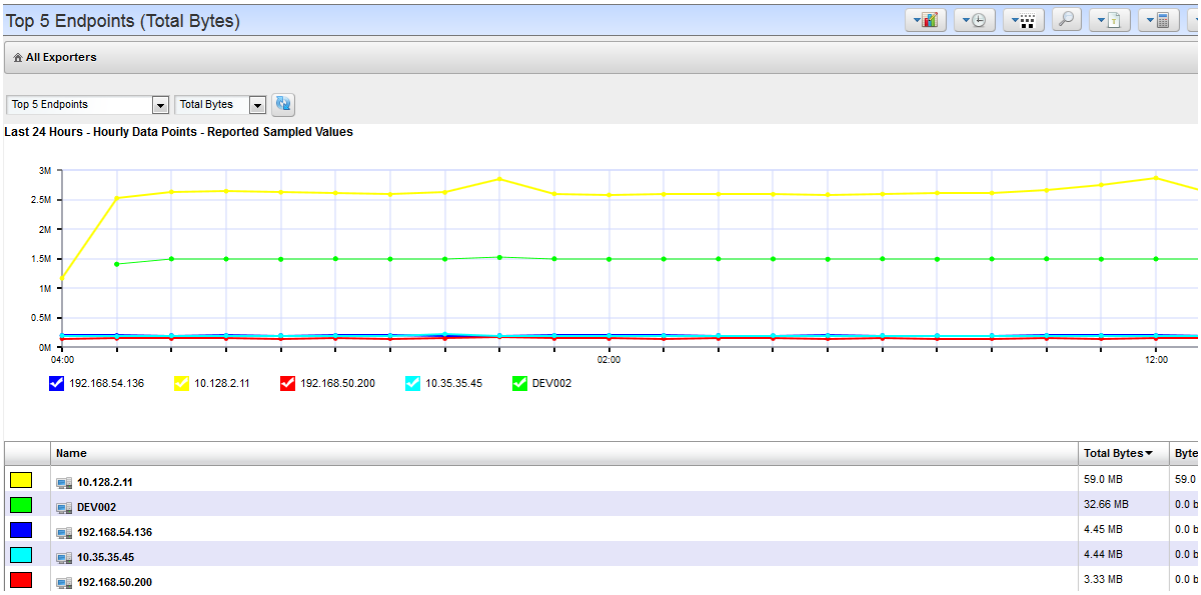
The Expanded Traffic Flow Portlet displays an interactive graph. You can also Drill Down to details about components within this portlet by clicking on one of the links in the table below the graph.

NOTE:

The selected period determines whether data is present, especially if you have just started monitoring Traffic Flow. Choose the shortest period to see data immediately (it still takes a few minutes to appear), and select longer periods only after monitoring has run for longer periods.

Expanded Traffic Flow Portlet

When you expand the portlet, a more complex interactive view appears. Initially, it displays a line graph for the selected time frame.

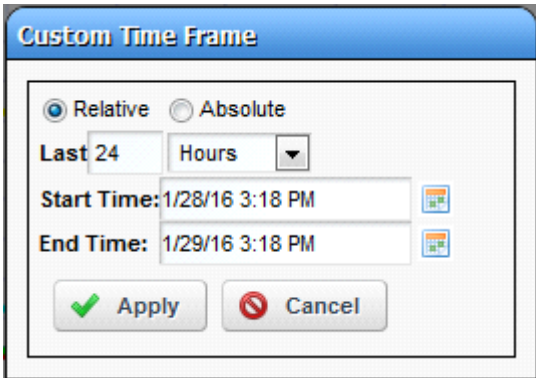


The graph on the upper portion of the portlet shows the data points for every time-slice and the chart below this graph shows the aggregate for all data points covering the selected time frame.

The following controls appear in the title bar:

Select Chart Type—Lets you change the chart type. Available chart types include *Pie*, *Line*, *Bar*, *Stacked Bar* and *Column*. Note that the pie chart only displays aggregate data while the other chart types display time-slice data within the selected time frame.

Select TimeFrame—Several built-in relative time frames are available including *Last 15 Minutes*, *Last Hour*, *Last 6 Hours*, *Last 24 Hours*, *Last 5 Days*, *Last 30 Days* and *Last 12 Months*. *you can also select Custom to display the Custom Time Frame popup screen.*



When this screen is shown, first select either Relative (wherein the time frame starts a certain period of time ago and includes everything up to the present) or Absolute (wherein the time frame includes everything between a certain arbitrary start time and end time that can both be in the past). If Relative is selected, you must enter a relative time value and time unit. For

example, Last 8 Hours, Last 120 Minutes, Last 45 Days, etc. If Absolute is selected, you must enter an absolute start and end time. Click Apply for these settings to take effect.

Data for Last 15 Minutes shows minute-by-minute data and this type of data typically appears after about 2-5 minutes of collection (after the exporter is first registered and flow packets are received from this device). Data for Last 24 Hours shows hourly data by default, and this type of aggregate data is computed after each hour has passed. For example, aggregate data for 9:00 AM will only be computed after the 9:00 hour has passed (9:59 AM has rolled over to 10:00 AM). Likewise, daily data is computed once the day has passed into the next (11:59 PM has rolled over to 12:00 AM). Changing the time frame displays time-slice data points, each of which represent a certain time range, such as a single minute of data or a full hour of data. The granularity of the time-slice data points is determined initially by the length of the selected time interval, but you can then use the "Select Granularity of Data Points" option to display different time-slice data points for the same time frame.

The granularity of time-slice data points is determined initially by the length of time frame (the duration from the start time to the end time), according to the following thresholds:

Less than or equal to 60 minutes: 1 Minute data points

Less than or equal to 12 Hours: 10 Minute data points

Less than or equal to 3 Days: Hourly data points

Less than or equal to 30 Days: Daily data points

More than 30 Days: Weekly data points

Select Granularity of Data Points —Lets you change the granularity of the time-slice data points that are shown in the graph. The options for granularity are 1 Minute, 10 Minute, Hourly, Daily, and Weekly. The way this works is that the less granular data (representing longer time intervals) are aggregates of the more granular data. For example, a 10 minute data point representing 6:20 would be an aggregate of all 1 minute data from 6:20 to 6:29. Likewise, an hourly data point from 6:00 would be an aggregate of all 1 minute data from 6:00 to 6:59. When you select a time frame, the length of the interval determines the granularity of the data points that are shown at first, but you can change this. For example, the time frame Last 24 Hours will by default show hourly data points, but you can then see more granular data by selecting 10 Minute from this menu. It would even be possible to show 1 Minute data for this same time frame, but this might cause the web browser to perform poorly because there would be hundreds of data points.

Search—Displays a search dialogue to find specific traffic data.

Select Report Type—Lets you change the number of results that are shown and also whether to show the most or least significant results. You can choose between Top 5, 10 or 25 and Bottom 5, 10 or 25.

Select Mode of Calculation — Lets you change the mode of calculation for data values. NetFlow and sFlow data are often sampled, which means that the values reported by the exporters should be understood as representing only a fraction of the total traffic. You can choose to show either the reported sampled values or the estimated total values. The estimates are calculated by multiplying the sampled values by the sampling rate, as reported by the exporter in one of the following ways:

- sFlow sampling, where the sampling rate is in the packet (usually 512 or 1024 or some power of 2)
- NetFlow V5, where the sampling rate is in the header of the packet

- NetFlow V9 with a single sampling rate for the entire device. In these cases an options datagram contains the sampling rate for the device.
- NetFlow V9 with a sampling rate specific to an interface. In these cases an options datagram contains a sampling rate and a sampler ID. Flows then contain a sampler ID to associate to this. When flows say the sampler ID is 0 then this feature is disabled for this interface.

Estimated total bytes and packets are calculated by multiplying the reported sampled values by the sampling rate. This works differently for sFlow and NetFlow. NetFlow packets contain fields for the reported sampled bytes and packets. For example if the packet reports that the sampled bytes is 45 and the sampling rate is 100 then the estimated total bytes will be 4500. Likewise if the sampled packets is 3 then within this same example the estimated total packets will be 300. sFlow packets do not contain fields for the sampled bytes or packets. Instead, sFlow works by sampling packets that are going through the exporter, and attaching these sampled packets to sFlow packets for export. So the reported sampled bytes is computed by adding the total bytes of the sampled packet that is contained within the sFlow packet and the reported sampled packets is naturally 1 for each sFlow packet that is exported. The estimated total bytes and packets is computed by multiplying each of these numbers by the sampling rate that is reported in the sFlow packet. For example, if the sampled bytes is 10 and the sampling rate is 512 then the estimated total bytes will be 5100 and likewise the estimated total packets will be 512 since this is the sampling rate.

NOTE:

For devices that are not sampling traffic data (they are reporting on 100% of the traffic going through the device), the estimated values will be the same as the raw values.

Traffic Flow Snapshots— Load or save a snapshot (preserved views) of traffic flow.

Export Data—Lets you export the data in the current view to a file. You can either save the current view to a PDF file or export the data to a CSV file. If you select Export to PDF, the resulting file will show a screen shot of the graph and the chart as shown on the screen. If you select Export to CSV, the resulting file will contain the data points for the time-slice data in the graph shown on the screen. The exception to this is if you are viewing a pie chart - in which case there is no time-slice data and the file will instead contain the same aggregate data as shown in the chart that appears on the screen below the graph. You can retrieve the generated file in the *My Alerts* area at the lower left corner of the portal.

NOTE:

When you export a line graph to CSV, the resulting file will have the times (minute-by-minute, hourly, etc.) in the header row, but the spreadsheet program you are using (i.e. Microsoft Excel) will apply default formatting to these values. You can apply your own custom formatting as needed.

NOTE:

The Export to PDF menu item is not available when canvas based line charts are enabled. If you need to use this feature turn off Canvas Line Charts in the Application Settings.

Settings—Allows you configure the way OpenManage Network Manager stores and queries traffic flow data. You can configure how to retain data, based on collection / rollup intervals.

Below the title bar a navigation bar displays the context path. See Drill Down on page 253 below, for more about this.

Below that navigation bar a row containing the following controls appear:

Entity Type—Selects the type of entity to report on (Exporters by Equipment Manager, Exporters by Subcomponent, Applications, Conversations, End points, Senders, Receivers, Autonomous Systems, and Protocol).

Attribute—Selects which attribute to graph (Bytes, Packets, Bits/Sec).

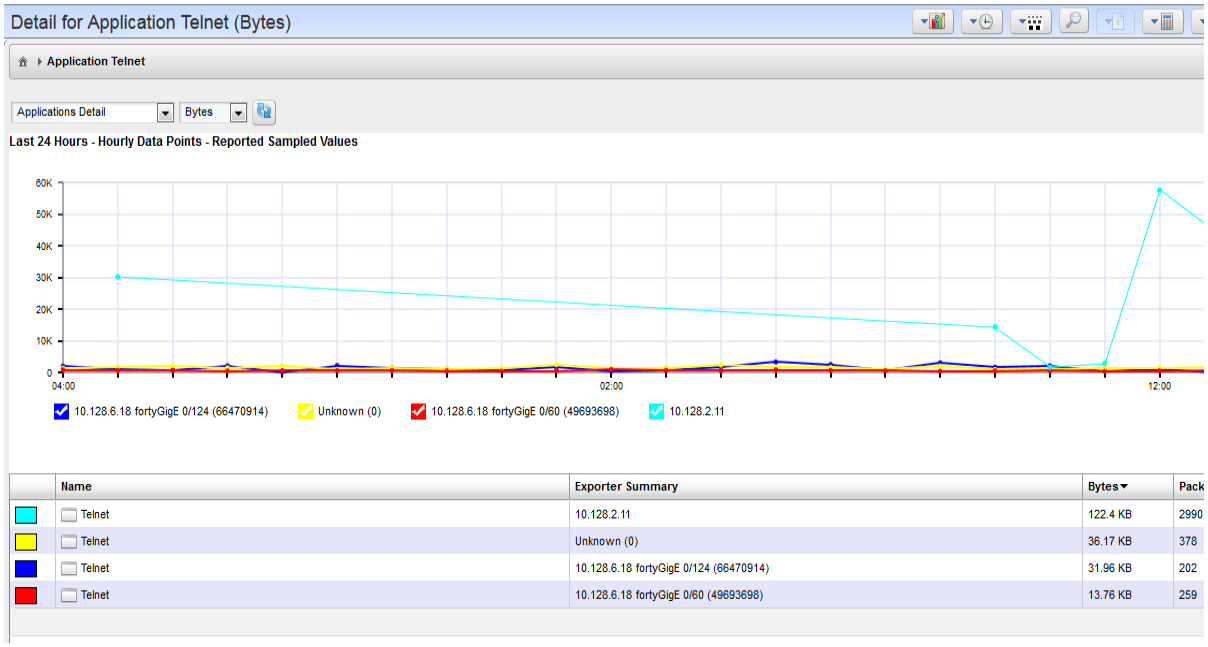
Refresh—Refreshes the screen (runs the report) applying any new settings.

NOTICE

You can check / uncheck by clicking on the colored squares in the legend below these graphs. This reveals / conceals lines connected to the labelled item.

Drill Down

you can “drill down” into a report by clicking on one of the links in the table. This displays a detail view of the selected entity and the name of the entity appears in the navigation bar.



When a detail view appears, the entity type appears as in the title bar. You can change to a “Top / Bottom n” report of a different type, then click refresh to display a report of the top entities that apply to the current detailed entity. Each time you click into the detail view for an entity, this adds the entity to the context, so that the report is generated by applying all of the filters that have been added to the context.

When you add an entity to the context, there will be fewer entity types available in the drop down list. For example, if you start from Exporters by Equipment Manager and then click on the name of an equipment manager in the list, this will then add this entity to the context. If you then change the entity type to Exporters by Subcomponent, then only the subcomponents within this equipment manager that are also flow exporters will be shown. Keep in mind that you might have to change the flow direction option to "Both Ingress and Egress" for all possible subcomponents to show in this view. You could then change the entity type to another available option such as Applications, Protocols, etc. for a more detailed look at what flows are going through the selected exporter. Another way of drilling down is to start with something other than an exporter, such as

Senders, Receivers, etc. and clicking into the detail view for a specific entity that is shown in that view. There are many permutations of drilling down into different entity types that will work to show exactly what you are interested in. This process can continue until the Conversation Detail view is reached. This is the end of the line for drilling down.

Search

Search by clicking on the Search (magnifying glass) icon in the title bar. Type any string in the next screen to search through the traffic data. A list of all entities found matching the string appears below it.



Entity found in the search support the following actions:

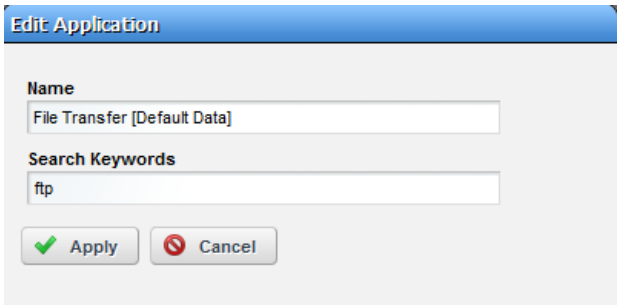
View Top Conversations—Displays the top n conversations for the selected entity.

Show Detail View—Displays a top level detail view of the selected entity.

Add to Current View—Adds the entity to the current view and drills down to it.

View TOP Conversations — Displays the top n conversations for the selected entity.

Edit — Allows you to edit information about the entity. This is currently only supported for applications. If you click this icon then another screen will be shown that allows you to edit the name and/or the keywords of the application.



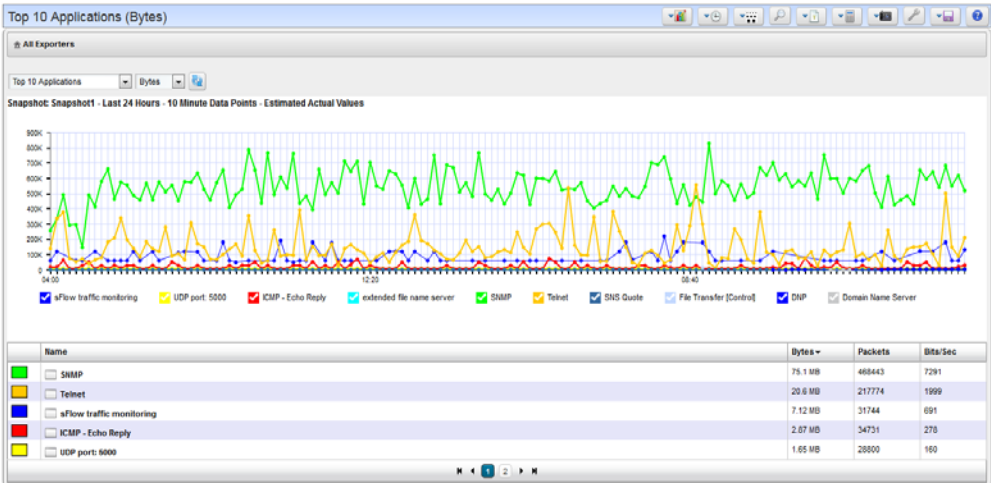
This is useful if you have a custom application that has traffic flow data associated with it. By default, the names for such applications has the format "(prototol name) port: (port number)". For example "UDP port: 5001". If it is the case that you see an application entry that has this default name or has the wrong name and you would like to change it, you can do so through this screen. Also you can enter keywords that will help with future searches. Click Apply to save the changes and return to the search screen.

NOTICE

The *Settings* button (the gear in the upper right corner) lets you confine the search by types (*All, Applications, Protocols, Autonomous Systerms, Endpoints)).* Note that you cannot search by exporters through this screen. If you select one of the two items for exporters in from the entity type drop down list, then this will show a paginated list of all exporters (by equipment manager or by subcomponent, depending on which item was selected). If you want to search for a specific exporter by equipment manager, then you can go to the Managed Resources portlet and use its built-in searching capability and then use the menu item to Show Traffic as Exporter. Likewise if you want to search for a specific exporter by subcomponent, then you can go to either the Ports or Interfaces portlet (both are different types of subcomponents) and also use its search capability and menu item to Show Traffic for the subcomponent entity.

Traffic Flow Snapshot

This portlet lets you display Traffic Flow you configure and save as a snapshot in a portlet visible on any OpenManage Network Manager page. It is, in effect, a portlet that permanently displays the Expanded Traffic Flow Portlet, beginning with the selected snapshot.



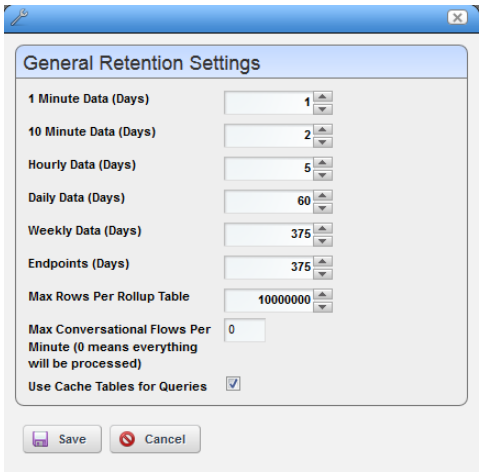
After adding this portlet to a page, use the selector to choose which snapshot you want to appear. Refresh the portlet with the double arrows to the right of the units displayed. You can also change what appears, the units, the time interval, and so on, just as described in Expanded Traffic Flow Portlet on page 250.

Settings

You can edit the configuration options by clicking on the Settings (wrench) icon.

Several of the fields shown on this screen are for the number of days to keep each granularity of traffic flow data. Initially, all traffic flows are associated with a specific minute and thus become 1 minute data in the database. These flows then aggregate (rollup) to larger degrees of granularity. 1 minute data aggregates to 10-minute intervals, which aggregate to hourly, which aggregate to daily, which aggregate to weekly data. It is important to consider how long you need to keep each granularity of data and to set the values accordingly. If you are saving data for longer than you need it, then this can fill up your database.

On this screen there are also fields that help you optimize queries. You can set the maximum number of rows per rollup table, which can be helpful for improving query performance. Also you can determine whether or not the queries should use the cache tables. Using cache tables is faster, but there is a possibility that not all of the detailed flow data is in the cache tables, so it is sometimes helpful to un-check this box, which will use the raw data tables instead.



Sometimes the volume of traffic flow data collected from the exporters can overwhelm the database. OpenManage Network Manager collects traffic flow packets (sFlow, NetFlow, IPFIX) from the registered exporters and aggregates the data into 1-minute flows differentiated by exporter, protocol, application, and conversation (including sender and receiver for both IP and autonomous systerm). Every minute, these flow records are inserted into the database. The number of distinct flows, differentiated by each of these fields, can sometimes add up to more row inserts than the database can handle in a single minute. In such cases, the only way for the system to function is for it to only insert the conversation-based flows that are the most significant (highest byte totals) and allow for the less significant flows (low byte totals) to be aggregated into a single flow that represents all other conversations.

This can be done through the “Max Conversational Flows Per Minute” feature. This feature is disabled by default, but if enabled it will reduce the number of inserts to the database per minute while preserving the most significant flows and also while preserving the overall byte and packet totals. What this means is that if you enter a number for “Max Conversational Flows Per Minute” then you are configuring OpenManage Network Manager to keep that many flows per minute. So this many flows will be inserted into the database as differentiated by exporter (by equipment manager and by subcomponent), protocol, application and conversation (sender and receiver) but any flow above this number will lose their conversation data and will only be differentiated by the other three fields (exporter, protocol, and application). It does this by first ranking all flows by estimated total bytes and then taking the highest N and inserting each of these into the database as they were reported by the device. The rest of the flows are then aggregated into the “Other” category and inserted into the database.

For example flows with estimated total values of 3, 15, 44, 89, 248, 510, 746, 1038, 4313, and 9755 and "Max Conversational Flows Per Minute" of 5 would find the top 5 to be 510, 746, 1038, 4313, and 9755. These flows would have their sender and receiver data (IP and AS) saved in the DB but the values 3, 15, 44, 89, and 248 would be added together into the "Other" category, but their protocol, application, and exporter data would be preserved. So these smaller flows would only actually be aggregated if they were all for the same exporter, protocol and application.

To enable this feature, enter a value for Max Conversational Flows Per Minute. Enter the highest number of conversational flows that you believe your system is capable of handling per minute. Note that a value of 0 disables this feature so that everything will be processed.

Domain Name Resolution

Initially the Name column of senders, receivers, endpoints and conversations shows the IP address. There is a task that is configured to execute periodically to resolve these IP addresses to domain names. This works as long as a DNS server is available within the network. When an IP address is resolved to a domain name, this name is shown in the Name column when viewing senders, receivers, endpoints and conversations. By default, this task executes every 24 hours. To configure how this task is executed, navigate to the Schedules portlet and search for an item where the description contains the text "Resolve hostnames using DNS". From here you can edit the frequency of the execution of this task and you can also disable this feature if you wish.

There is also an option to perform this DNS lookup for public IP addresses but to exclude private IP addresses. To disable private IP DNS resolution while keeping this feature enabled for public IP addresses, add the following line to installed.properties and restart the application server:

NetFlowRetentionMBean.EnabledPrivateIPDNSLookup=false

You can also manually execute this task by navigating to the Actions portlet and searching for an item where the name contains "Resolve DNS Hostnames". From here you can execute this action on demand rather than waiting for the scheduled task to execute. When you execute this task manually, you have the option to re-do the DNS resolution for all endpoints, including those that were previously resolved. Caution: Executing this action with this option selected can be very time consuming and resource intensive.

Traffic Flow Analyzer - Example

The following describes typical situations where flow is useful. When ports are over-utilized because of intermittent performance problems diagnosis of the problem sometimes difficult. Turn on flow traffic data collection to evaluate who, what applications, and so on, are responsible for the traffic on the affected ports. This avoids getting overwhelmed with collection of traffic going in all directions. Follow these steps to do this:

1. From the Resources monitor, select a desired router that has support for NetFlow / sFlow
2. Enable NetFlow / sFlow on most impacted routers that support NetFlow / sFlow. Also, register a number of exporters to enable an efficient and scalable data collection environment.

NOTE:

You can disable NetFlow / sFlow and unregister exporters.

3. After NetFlow / sFlow has been running for a while, verify that bandwidth utilization is within expectation. This will help insure optimum performance of critical business applications.
4. Select the Top 5 Applications portlet (or add it to the page).

5 From the list of the Top 5 Applications, you'll typically see most bandwidth is being consumed by the key applications in our organization.

Alternative 1

6 To ensure bandwidth is not being hijacked by unauthorized or unwanted video or music streaming applications, select the Top 5 Conversations.

7 Often the top conversation is video streaming software.

8 To answer "Where and who is running this rogue application?," drill down into the conversation to see End points involved in the conversation. This identifies the user running the streaming application. You could now go and stop (or block) this rogue application.

Alternative 2

An alarm indicates port X is surpassing its threshold. If the port has become a bottleneck in the overall network bandwidth, we want to identify what applications are at cause, and who is responsible for running them.

1 Look in the Top 5 Traffic Flow Endpoints portlet.

2 From the list of the Top 5 Endpoints, you will typically see that port X is high on the list.

3 Expand the portlet and drill down into the port X endpoint to see what are the top conversations going through port X.

4 Drill down into conversations to identify any unauthorized applications.

5 Drill down further to identify users of any unauthorized applications

6 Now, go stop them!



How To:

Create a Traffic Flow Report

You can create reports based on traffic flow data.

1 Create a new Report Template by right-clicking the Report Templates portlet, selecting New > Table Template.

2 Name the report (here: Test Traffic Flow Applications Report).

3 Select a source in the Source tab. Here: Traffic Flow Analyzer > Traffic Flow Exporter.

4 Notice that the Select your inventory columns panel displays the attributes available based on your traffic flow entity type selection.

5 Select Available columns and click the right arrow to move them to Selected. Follow these guidelines:

- You should always select the entity name column (Exporter Name for the entity type Traffic Flow Exporter, Application Name for the entity type Traffic Flow Application, etc.) There are also certain entity type specific columns that provide context for the entity that is being reported on. For example, Traffic Flow Autonomous System has an available column for ASN and Traffic Flow Conversation has columns for A Endpoint and Z Endpoint.
- Each template should be for either time-slice data (where the data values represent a specific slice of time within the total time range of the report) or aggregate data (where the data values represent sums or averages across the entire time range). Some columns are appropriate for one of these but not the other.

- Templates for time-slice data should include the Time column and one or more time-slice data columns, including Bytes, Packes, and Bits/Sec. For certain entity types the available data columns might include the three of these aforementioned, with directional orientation "In" and/or "Out" and perhaps also "Total", which is the "In" and "Out" values added together.
- Templates for aggregate data should not include the time column because the time is understood to be the total time range of the report. Also aggregate templates should include one or more aggregate data column, which includes Bytes (sum), Packets (sum), and Bits/Sec (avg). For certain entity types there might be directional ("In", "Out", "Total") versions of these aggregate attributes.
- Note that time-slice templates should not include aggregate data columns, and aggregate templates should not include time-slice data columns.

6 Arrange the columns and fonts as you like in the Layout tab.

7 Save the template.

8 Right-click, and select New in the Reports portlet.

9 Enter a Name and Title for the report.

10 Notice that since this is the first report created since you made the Test Traffic Flow Applications Report template, that it is the Report Template already selected.

11 Select the desired filter conditions. Note that all traffic flow entity types have the same available filter attributes. If a value is not selected for an attribute then a default value will be used:

- Calculation Type defaults to Reported Sampled Values.
- Data Point Type defaults to Hourly.
- Report Limit defaults to 10. Note that only the Equals operator works for this filter condition.
- Report Limit Type defaults to Top.
- Direction defaults to both Ingress and Egress.
- Time defaults to Within Last 24 Hours. Note that the only comparison operators that work for this filter conditions are Within Last, Is, Between, and After.
- Exporter Equipment Manager is not specified by default (meaning that data for all exporters should be included), but this attribute can be used to filter by a specific exporter by equipment manager (which includes all subcomponents).
- Exporter Subcomponent is also not specified by default (again this means that data for all exporters should be included), but this attribute can be used to filter by a specific exporter by subcomponent (port or interface).

12 Test Traffic Flow Applications Report should appear in the Reports portlet.

13 Right-click and select Execute (noticing that you can also schedule such reports, even repeatedly).

14 Click the magnifying glass to the right of the Report Completed message in My Alerts to see the report.

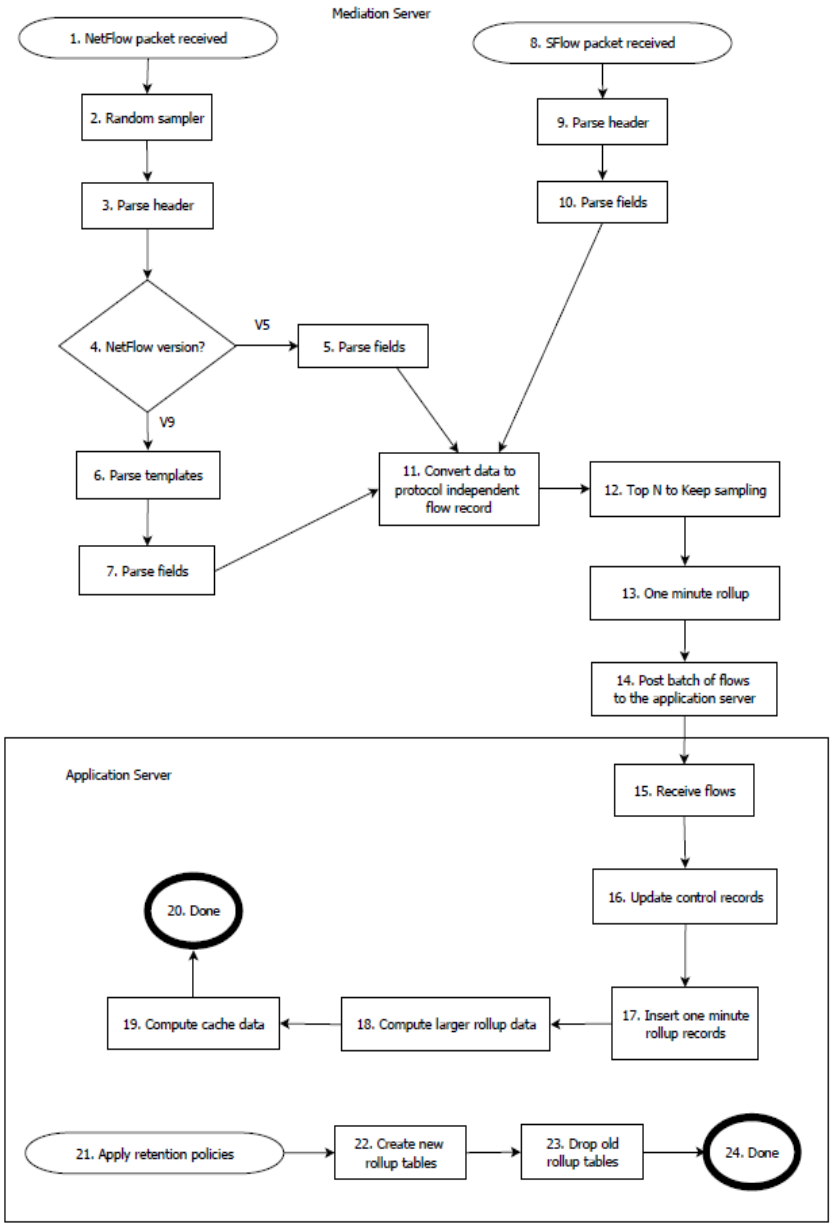
15 Hover your cursor over the lower right corner of the report to see a set of icons that let you expand, zoom out and in, save, or print the report.

NOTE:

Traffic Flow Analyzer doesn't support comparison reporting.

Traffic Flow Analysis Life Cycle

The following diagrams OpenManage Network Manager's Traffic Flow Analysis life cycle



Traffic Flow Analysis Life cycle Legend

1 **NetFlow packet received**—OpenManage Network Manager received a NetFlow packet from a registered exporter. OpenManage Network Manager ignores NetFlow packets from devices not registered as exporters.

2 **Random sampler**—OpenManage Network Manager applies random sampling to incoming packets. This currently applies only to NetFlow packets and not sFlow packets. The `NetFlowListenerMBean` attribute `SamplingRate` (1 by default) determines this behavior.

   This value represents the average number of packets received before one is processed (the others are discarded). If `SamplingRate` is 10, then OpenManage Network Manager processes one of every 10 packets on average and discards the other nine. The default processes every received packet and does not discard any (at this step).

3 **Parse header**—OpenManage Network Manager parses the NetFlow packet header. The header contains information like its version and the number of flows it contains.

4 **NetFlow version?**—Determines the NetFlow packet version (V5 or V9).

5 **Parse fields**—Fields for a NetFlow V5 packet are determined by a standard template and parsed here.

6 **Parse templates**—For NetFlow V9 packets OpenManage Network Manager must find the template that the packet header references. OpenManage Network Manager receives templates as NetFlow packets from the same exporter sending flow packets. If OpenManage Network Manager has not yet received the referenced packet yet then it sets the current flow packet aside until the template comes in. When that template comes in, it is parsed (there is a standard format for template packets) and then TFA will know how to parse the flow packets that reference it.

7 **Parse fields**—OpenManage Network Manager parses the fields of this flow packet using the header-referenced template.

8 **sFlow packet received**—OpenManage Network Manager received an sFlow packet from a registered exporter. OpenManage Network Manager ignores sFlow packets received from devices not registered.

9 **Parse header**—OpenManage Network Manager parses the header of the sFlow packet. The header contains information like the version and the number of flows contained within the packet.

10 **Parse fields**—OpenManage Network Manager parses the fields of this packet according to the standard sFlow template.

11 **Convert data to protocol independent flow record**—TFA supports multiple traffic flow protocols (NetFlow, sFlow) but once OpenManage Network Manager parses the data within these packets, it does not depend on any specific protocol. Here, OpenManage Network Manager normalizes data into protocol-independent flow records.

12 **"Top N to Keep" filtering**—OpenManage Network Manager applies the "Top N to Keep" filtering here. This feature lets you set a maximum number of conversational flows per minute to keep, which in turn means that if OpenManage Network Manager receives more than this number in any given one minute period, then it aggregates the rest into the "Other" category. OpenManage Network Manager ranks the received flows according to the number of estimated total bytes they report on and preserves all data only for the flows designated most significant by this measurement. It still preserves the total byte and packet data for the less significant flows, but the sender and receiver will be set to "Other".

   The NetFlowListenerMBean attribute ReceiverTopNToKeep determines the number of flows to keep. This is zero (0) by default, turning this feature off, which means the system will fully processes conversational data for all received flows.

13 **One minute rollup**—OpenManage Network Manager collects and "rolls up" (aggregates) flows by conversation and at the end of every minute submits the resulting one minute rollup flows for further processing.

14 **Post batch of flows to the application server**—Most of this processing occurs in the mediation server (process or host). Once OpenManage Network Manager produces the normalized, protocol-independent flows, it adds them to a queue the mediation server posts to the application server. Once the application server receives these results, it inserts them into the database for later querying. You can monitor this queue through the JMX console > oware > service=NetFlowListenerMBean and the operation getQueueCount.

15 **Receive flows**—The application server receives flows from the mediation server.

16 **Update control records**—Every flow refers to control data, which includes the IP address of the sender and receiver, the AS number of the sender and receiver, the protocol and the application. OpenManage Network Manager updates the associated database records here.

17 **Insert one minute rollup records**—OpenManage Network Manager inserts the one minute rollup flows into the database so they can be queried later.

18 **Compute larger rollup data**—The one minute rollup records contribute to larger rollup records, including those representing 10 minute, hourly, daily and weekly time intervals. At the end of every time interval TFA computes the appropriate rollup records.

19 **Compute cache data**—Sometimes the volume of data can be so high that queries summarizing it can take several minutes. To make querying more efficient, OpenManage Network Manager summarizes the data ahead of time and caches the results in the database.

20 **Done**—Done processing new traffic flow data.

21 **Apply retention policies**—Apply retention policies to add new rollup tables and/or drop old rollup tables.

22 **Create new rollup tables**—OpenManage Network Manager creates new rollup tables as necessary according to the settings in NetFlowRetentionMBean as specified in the attributes rolloverFrequencyValue1Min, rolloverFrequencyValue10Min, rolloverFrequencyValueHourly, rolloverFrequencyValueDaily and rolloverFrequencyValueWeekly.

23 **Drop old rollup tables**—The old rollup tables are dropped as necessary according to the data retention settings that can be edited by clicking on the wrench icon from the expanded TFA portlet.

24 **Done**—Done applying retention policies.

10

Actions and Adaptive CLI

The Actions Manager lets you manage actions like enabling monitors, file backups, resyncs and so on. These actions are typically limited in scope, and not that complex. On the other hand, it also manages Adaptive CLI (command-line interface) commands to run against devices which can be complex.

These commands amount to "mini-scripts" to query and configure those devices. In it, you can create commands to run against devices after the device driver has opened a connection to the devices. The driver handles logins, and general connection management. You can even initiate these actions with the application's actions that target groups (see Discover Links for a Group of Devices, for example)—although if you delete a target group, such operations fail. Many drivers seed pre-configured command that appear listed when you first open this manager. For a brief overview of creating and using these, see How to: Create Adaptive CLI Examples on page 293.

Adaptive CLI's Attributes capabilities let you insert variables in scripts. See Attributes on page 272 for the details. You can also assemble configurations made here as component Tasks to execute with other component Tasks. You can even use this capability to include Perls scripts within OpenManage Network Manager. See Perl Scripts on page 291.

NOTICE

You can have Actions maintain lists like ACLs, and when these change, in the Adaptive CLI script, push the updated list out to the appropriate devices.

Adaptive CLI commands let you map several vendor-specific commands to a single action, so you could, for example, query two types of devices throughout the network for their MAC addresses with a single action. Adaptive CLI actions can also help you debug more complex scripts that either query or configure devices.

The Adaptive CLI manager displays a list of *Configure* and *Show* commands (the *Command Type*) with a *Name*, *Description* and the *Last Run Date*. You can filter what appears in this manager with the fields at its top.

NOTE:

The contents of the Action Portlet vary, depending on the installed options in your package.

CAUTION:

Particularly for Adaptive CLI, and possibly for other OpenManage Network Manager capabilities, the level of access to devices must match the desired effect. If OpenManage Network Manager's login to a device permits only read access, then Adaptive CLI configuration commands which require write capabilities will not be effective.

Using Adaptive CLI

You can quickly take a set of commands or configuration file snippet from a device, copy it directly into the Script editor, mark it up, and save it as a working CLI.

When using the CLI Format, The Adaptive CLI tool will prompt you to create new attributes based upon your script markup. This lets you quickly create a script and schema to create an ACLI. If you have attributes that are mainly simple String attributes, this is a very quick and automated approach.

Using Perl in Adaptive CLI

If you need conditional logic that goes beyond simple scripting, you can use Perl in Adaptive CLI. The example below checks to see if a String Attribute is empty (null) or not. If the String attribute (`ShowCmdString`) has content, the show command with `ShowCmdString` as a parameter goes to the device. Otherwise, the Perl script skips or excludes this statement.

Embedded CLI Example:

```
[IF ShowCmdString]
Show [ShowCmdString]
[ENDIF ShowCmdString]
```

You could use the CLI format for the above example, but if you need to check attributes of other types, besides String, then you must switch to Perl. For example:

Boolean `myFlag` equals True:

```
if ($myFlag)
{
     …
}
```

Integer `myInt` greater than zero:

Example:

```
if ($myInt > 0)
{
     …
}
```

To check whether a string is a particular value—like from a valid values list entry assigned to the String attribute—then you must also use Perl. The CLI format only can test if the String exists. It cannot validate its value when populated. For example: EncapsulationType = “VLAN-CCC”, “VLAN-TCC”, … You can not do this check with the CLI Format: `[IF EncapsulationType = “VLAN-TCC”].` Instead, use a Perl script with a statement like this:

```
If ($EncapsulationType  eq  “VLAN-TCC”)
{
     print “set encapsulation $EncapsulationType\n”;
}
```

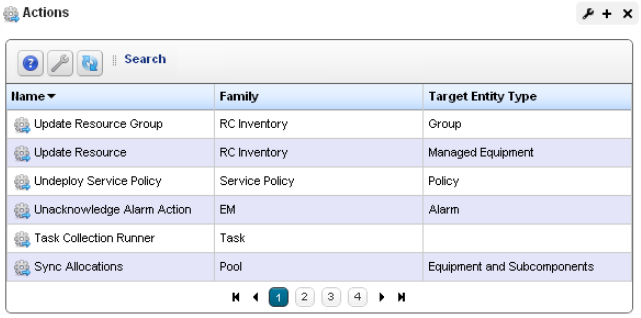
If any attributes in your script are a List (Collection), the only way to loop through the list’s items during the Adaptive CLI execution is to use Perl. For example: Processing a List of Strings:

```
$count = 0;
foreach @MyCommandList)
{
   print (“$MyCommandList[$count]\n”);
   $count++
```

}

Actions Portlet

The Actions Portlet lets you manage actions like Adaptive CLI, backups, change management actions, and so on. The list of actions available to your system depends on the exact configuration you have installed. This portlet is the primary access point for Adaptive CLI editing.



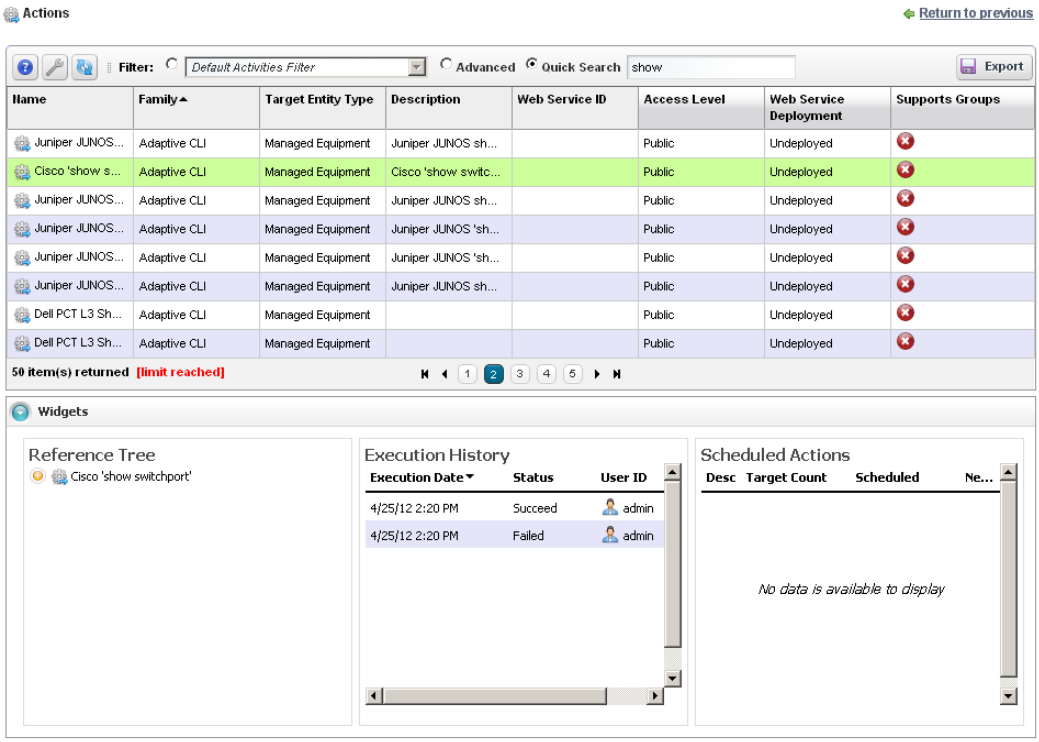
The summary portlet displays columns with the *Name*, *Family*, and *Target Entity Type* for the listed Action. The Family column describes the type of Action. Right-click and select *New* > *Adaptive CLI* to create a new action. You can also import/export actions and share actions with other users on your system.

CAUTION:
For Adaptive CLI to be fully functional, you may need to install it on your servers. Refer to the *OpenManage Network Manager Installation Guide* for Perl installation instructions.

To configure and schedule groups of actions, right-click in the Schedules portlet, and create an *Action Group*. This lets you run several actions, and configure their order and targets.

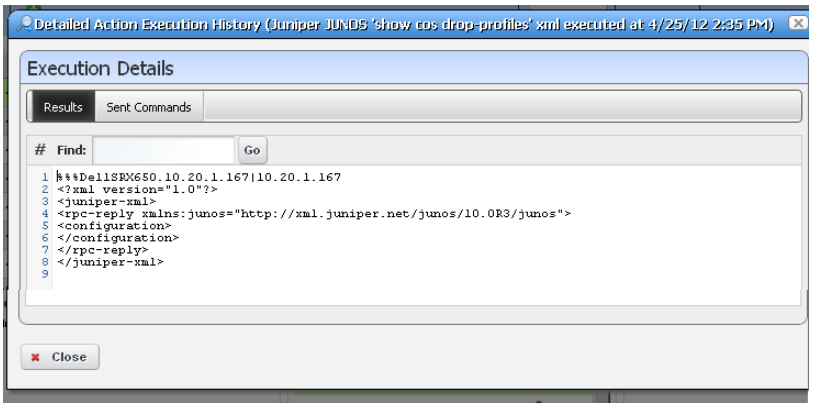
Expanded Actions Portlet

The expanded portlet has the same right-click menu as the summary portlet, and adds columns for *Description*, *Last Web Service ID*, *Access Level*, *Web Service Deployment*, and *Supports Groups*.



The expanded portlet also has snap panels to display Reference Tree connections between the selection and other elements within OpenManage Network Manager, as well as an Execution History panel listing *Device Name*(s), *Execution Date* and *Status* for the selected Action, and a Scheduled Actions panel cataloging any Schedules for the selected Action. Right-click a Schedule to edit, execute or delete it.

The Execution History snap panel displays history by device. Right-click to see the details of what occurred when the selected action ran against a particular device (*Execution Details*).



The Execution Details panel displays tabs showing the *Results* of running an Adaptive CLI, and the *Sent Commands*.

You can also *View Job* to see a screen like the Audit Trail Portlet on page 630, or Delete to remove a listed Action record from the list.

Right-click menus on the Actions portlet can include the following items (these vary, depending on the Action's family):

New / Edit —Lets you create or modify a selected action in the Adaptive CLI Editor, described below. You cannot modify system-supplied Adaptive CLIs, but you can edit any that you create.

Execute—Execute the selected Action. This typically displays a target equipment selector screen, and a screen where you can configure any parameters necessary for execution, then a screen like the Audit Trail Portlet on page 630. OpenManage Network Manager validates the parameters before executing the Adaptive CLI. If a parameter is invalid, for example a blank community name in the Juniper Community Adaptive CLI, OpenManage Network Manager logs a validation error to the audit trail. In this case the Adaptive CLI is not executed and leaves behind no history record.

Some Adaptive CLI scripts also let you *Preview* what is sent the device in a subsequent screen. This does not appear in the execution of Targetless, and Multi-target Adaptive CLIs. Some actions are configured to target groups, too.

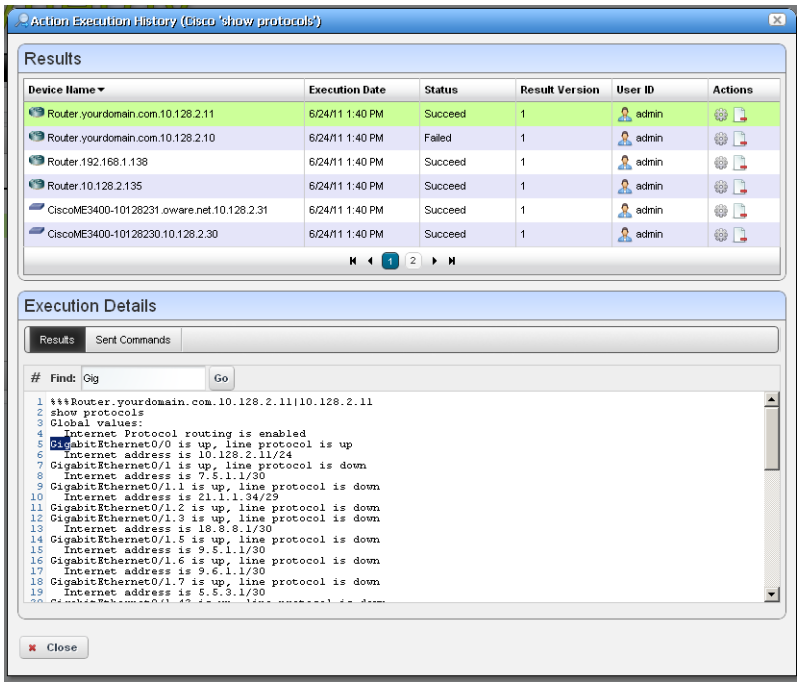
Details—Opens a screen displaying the Reference Tree, Execution History, and Action Details for the selected Action.

Web Services—You can elect to *Deploy* / *Undeploy* or *Export WSDL* to create a web service from the selected Action.

Deploy / *Undeploy Web Service*–Deploy or undeploy the selected activity as a web service. See Web Service Deployment Features on page 318 for more. Refer to the *Web Services Guide* for detailed information.

Export WSDL–This exports the WSDL for the selected activity. You must select the file name and location. Web Services Description Language (WSDL) is an XML format for the description of network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. See Web Service Deployment Features on page 318 for more.

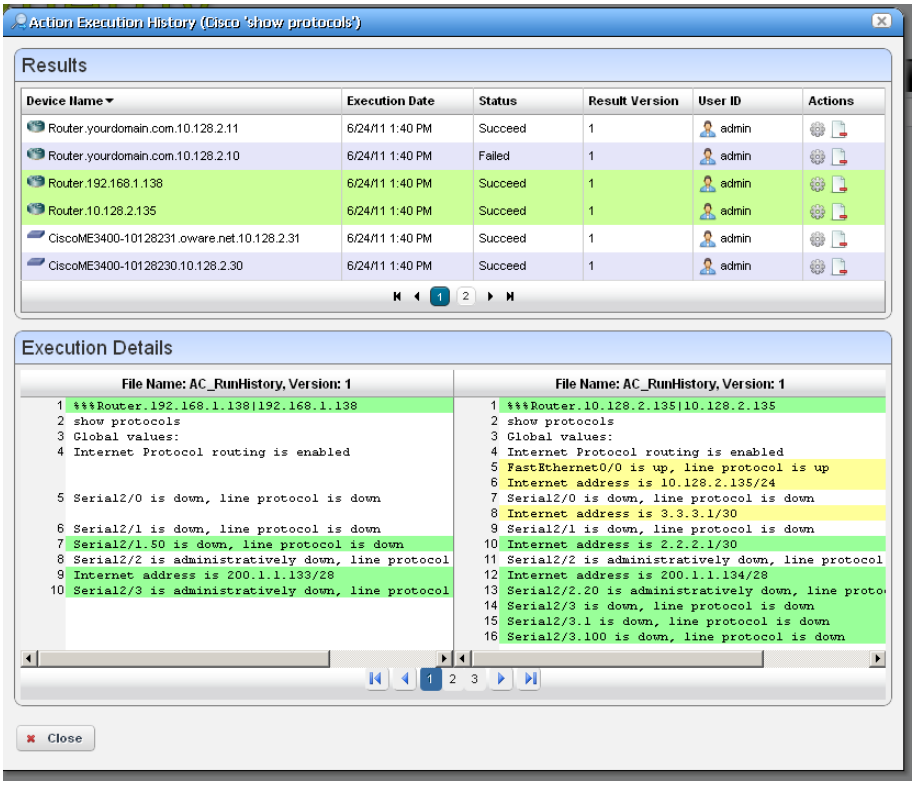
History—Displays the history of the selected action.



In the *Results* (top of screen panel) click to select the device for which you want additional information, and the *Execution Details* panel displays the *Results* of execution in one tab and the *Sent Commands* in another.

Notice that you can *Find* text within a result (click *Go* to repeat the find). You can also see the bottom panel if you right-click a single execution within the *Execution History* snap panel in the Expanded Actions Portlet.

If you select two executions in the top panel (or in the *Execution History* snap panel and right-click), a comparison appears.



This has the same color coding as you would see comparing configuration files. Lines that differ between the two Adaptive CLI results appear highlighted green. Lines that are missing in one, but that appear in another appear highlighted red. Added lines appear highlighted in yellow. Use the right/left arrows or the page numbers at the bottom of the screen to page through the side-by-side comparison.

Audit—Opens an Audit Trail Viewer for the selected Action. See Audit Trail Portlet on page 630 for details.

Show Last Results—Show the last execution details (like history for a single run).

Schedule—Schedule the selected Action. See Scheduling Actions on page 307 for details.

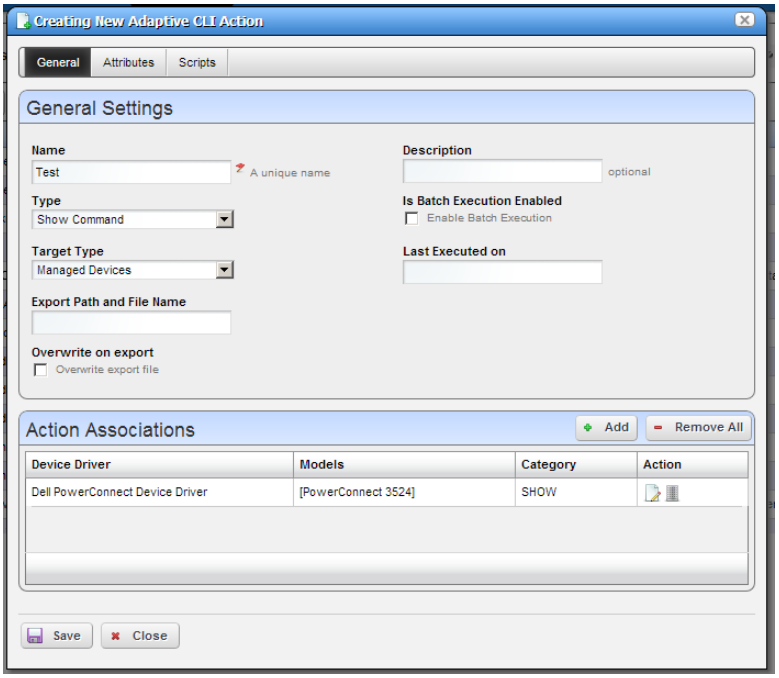
Delete—Remove the selected Action from the list.

Import / Export—Import or Export a file representations of the ACLI action selected. Best practice is to export single actions, or actions that share a Schema, rather than exporting all actions at once.

If you have multiple ACLIs sharing the same Schema, and change that Schema best practice is to retest the other ACLIs using that schema to ensure no unintended side effects occur.

Adaptive CLI Editor

This editor creates new Adaptive CLIs When you click *New*, or *Edit* after, selecting an existing command, the command editor screen opens. You can create *Configure Commands*, *External Commands*, and *Show Commands*.



The editor screen has the following tabs (the ones that appear depend on the type of command you are editing):

- General
- Attributes
- Scripts

The Adaptive CLI Manager logs into devices in enable mode by default. For most configuration commands (and even some show commands), you must typically first set the device to its configuration mode. For example: The first Adaptive CLI Manager command must be `config t` (Juniper E-Series) or `edit` (Juniper M/T series) to initiate the router's config/edit mode. OpenManage Network Manager also validates entries. If saving fails, a red "X" appears next to required omitted entries.

Click *Save* to preserve the Adaptive CLI you have configured. Clicking *Close* does not save your configuration.

General

The following are parameters to configure in this panel:

Name—A unique identifier for this action. For example: "Retrieve MyDevice MAC addresses."

For a new action to appear on the right-click Action menu, begin its name with the vendor name. For example, *Force10-showversion* would appear under Actions in that menu. Otherwise, it appears under and Adaptive CLI classification.

Description—A text description of the action.

Type—Select a type from the pick list (*CLI Configure Command*, *External Executable* or *CLI Show Command*).

The *External Executable* command refers to a script. Making this an ACLI means OpenManage Network Manager can schedule such scripts or include them in a workflow. See External Executable on page 284 for more about these.

NOTICE

You can use OpenManage Network Manager's optional Proscan policies to scan the results of Adaptive CLI show commands for compliance, and trigger actions (alarms, e-mail, and so on) based on their contents. See .

Target Type—Select a type of target from the pick list (*Card*, *Equipment and Subcomponents*, *Interfaces*, *Managed Devices*, *Ports*). Adaptive CLI targets can also be *None* (*Targetless*). On execution, if you create an Adaptive CLI type with port target, then the selection view panel lets you choose ports. When the Adaptive CLI type is *External* then Target Type can be *None*; otherwise it is not an option

If you want the target to be a OpenManage Network Manager group after you right-click an Adaptive CLI, and select *Execute*, select *(Group Membership)* in the target selector filter. Click the icon to the left of the *Go* button, and to the right of the empty field to see available groups. Select the group(s), and click *Done*. Click the *Go* button. Control click if you want a subset of the group's devices, or simply click *Add All* and then click *Done*.

Export File Location—This is a file name and path (`C:\mypath\myfile.txt`) where you elect to store the result of an adaptive CLI execution. You must specify an extension for the file, and may specify the variable `$IPAddress` in the filename for pattern substitution.

Overwrite on Export—Check to overwrite the result file. This overwrites any existing results file with new results (if checked). If it is unchecked, any new results append to the exported file, with a time / date stamp and target-identifying information.

Is Batch Execution Enabled—Check to allow consolidation of related Adaptive CLI scripts, provided the associated device driver supports such consolidation when provisioning a service. (Currently supported by the Juniper JUNOS driver only.)

Batching is valuable for instances like the following: if an Adaptive CLI-provisioned service has 10 sub-services, OpenManage Network Manager runs commands for the first service, then if it's successful, commits, and logs off. Then OpenManage Network Manager repeats this procedure nine times more, logging on, committing and logging off for each command. If batching is turned on, then OpenManage Network Manager sends the 10 Adaptive CLIs to the device as a single unit before committing and logging off. (This logic does not apply if you are running a procedure against 10 devices.)

Batching is best practice for Juniper devices, since if one line of a command fails, the device rolls back the entire block of commands. Cisco devices typically skip and do not commit failing lines.

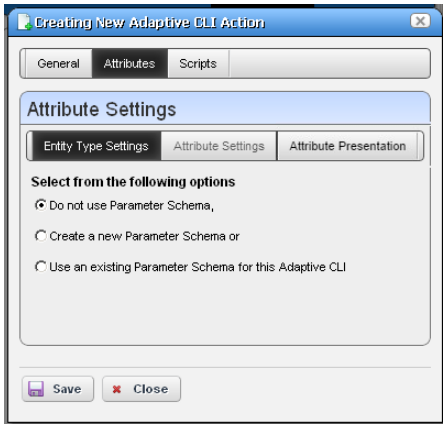
Last Executed On—Displays the last execution date. This is blank for new Adaptive CLIs.

Action Associations

Click the *Add* button to add associations to vendors and device models. For example, you can confine an Adaptive CLI to Dell devices, even to certain Dell models. When you right-click your discovered Dell device in the Managed Resource portlet, the associated Adaptive CLIs appear listed among the available actions you can request.

Attributes

Adaptive CLI commands let you configure modifiable *Attributes* as part of the command you send to the selected equipment.



Entity Type Settings

Use the radio buttons to select from the following options:

- Do not use Parameter Schema
- Create a new Parameter Schema
- Use an existing Parameter Schema for this Adaptive CLI

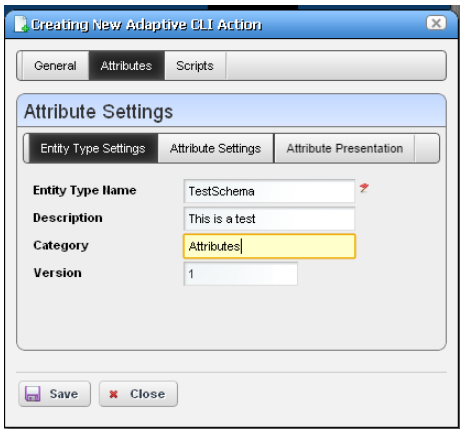
Sharing a schema rather than creating a new one with each Adaptive CLI lets you use the same attributes in complementary scripts. For example one script may create an entity, while another removes it. In this case, the valid values, labels, and so on for the attributes are always going to be the same in both create and delete Adaptive CLIs. This means sharing the same schema is both safe and easy. Either script can mark unused attributes as "Not applicable."

Do not use Parameter Schema

This option does not save a set of standard attributes to re-use later. Go directly to the Scripts tab to create this type of Adaptive CLI.

Create a new Parameter Schema

Click the *New* button and the schema screens appear.



Entity Type Settings

The *Entity Type Settings* tab has the following fields:

Entity Type Name—An identifier for the schema.

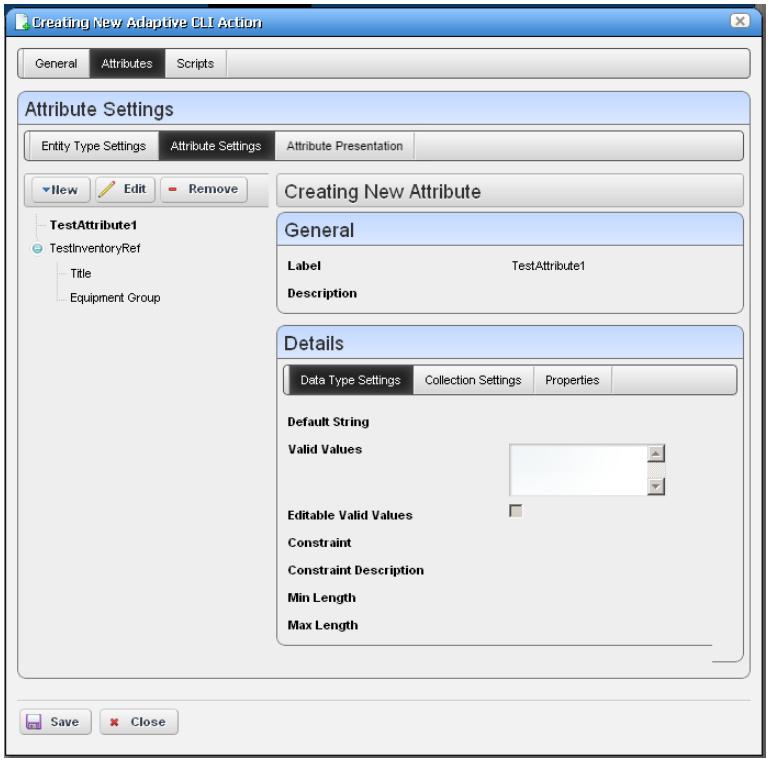
Description—A text description for the schema.

Category—A category for the schema.

Version—An automatically-created version number.

Attribute Settings

Click the *New Attribute* button and select the attribute type and open editor panel and configure



the attribute. Configured attributes appear in a tree to the left of the editor panel. Click a listed attribute to edit it after it has been created.

The editor panel has the following fields:

Label—An identifier for the attribute. These can have spaces, but not underscores, unless your package is 7.2.3 or later, which supports both.

Description—A text description for the attribute.

The following tabs may appear, depending on the type of attribute you are configuring (some are absent). Additional fields may appear, depending on the attribute type you are configuring:

Datatype Settings

Default Value—An optional default value for the attribute.

Collection Settings

Is Collection?—Check to classify this attribute as a collection.

Allow Duplicate Values—Check to enable allowing duplicates.

Allow Reordering—Check to enable allowing reordering.

Collection Min / Max Length—Enter the minimum/maximum number of characters in this attribute.

Properties

Upper / Lower Case—Check to validate on case.

Case Insensitive—Validation ignores case.

Multi Line Text—Check to enable multiline text.

One Way Encrypt—Check to encrypt.

Truncate—Truncate the attribute.

Attribute Settings

You can create new attribute schemas. See Attribute Editor Panels below for information about different datatypes' fields. Once you create a set of attributes, they remain available for re-use as a schema, or collection of attributes. To identify schemas, enter the following fields:

Label—A unique, mandatory identifier for the collection of attributes.

Description—A text description of the entity.

Click *New* to create or select an attribute in the displayed tree and click *Edit* to open an editor where you can create or modify attributes. Select an attribute and click *Remove* to delete it from the list.

Attribute Editor Panels

The following panels appears, depending on the attribute type selected from the pick list. The fields in the editor depend on this selection. Available types include *Boolean*, *Coded Value*, *Date*, *Decimal*, *IP Address*, *Integer*, *Long*, *Inventory Reference*, and *String*. The following fields appear for each of these types (omitting redundant fields):

NOTE:

Configure the data type of an attribute before you save a task. After attributes are in Scripts, you cannot change the data type.

Boolean

Default Value—Check for *True*.

Coded Value

Default Coded Value—Enter the default coded value. If an attribute a Coded Value then enter valid values in the format of NUMBER:Display Label. For example:

10:Hello World

20:Hello Moon

Without this pattern a validation error appears. Coded values become a Drop Down (Combo Selection) at runtime containing the Display labels within it (like Hello World, Hello Moon). Selecting one gives the script the numeric value (If users select Hello World, the value the script gets is 10)

The default appears by default in this list of alternatives. Enter any other alternatives below this field in the *Valid Values*.

Valid Values—Enter a valid value in the line above the table of valid values, then click the green + to add the value entered to the list. Click the *Remove* icon (the red -) to delete a selected value. These must be formatted like the *Default Coded Value*.

Date

Default Value—Enter a default date, or use date icon to display a calendar where you can select one. Click off the calendar to make it disappear.

Valid Values—Enter valid date values above the list, and click the green plus to add them to the list.

Decimal

Default Value—Enter a single or range of default decimal values.

Constraints—Enter a range of acceptable numbers separated by a colon. For example, Constraints = 2:4096. At runtime, a field where you can enter numbers. validates that entered numbers are between 2 and 4096 when running the Adaptive CLI. If you enter a number outside this range, a validation message appears and the attribute name turns red. You can also include several numbers or ranges separated by the pipe (|) character. If you specify a range, the lowest number must be to the left of the highest number. For example 9:99|999:1010.

Valid Values—Enter valid decimal range values, and click the green + (the red - removes them). You can manage these as described in Coded Value above.

IP Address

See also Validating IP Address Variables on page 277.

Default Value—Enter a default IP Address.

Valid Values—Enter valid values as described in Coded Value above. Check *IP Mask*, *Subnet*, *Allow 32 Bit Mask*, and *Allow Any Valid Ip* in the *Properties* tab if you want the values entered to be those.

Editable Valid Values—Check to enable editing of default or entered IP addresses.

Integer

Default Value—Enter a default integer.

Constraints—Enter a range of acceptable numbers separated by a colon. You can also include several numbers or ranges separated by the pipe (|) character. If you specify a range, the lowest number must be to the left of the highest number. For example 9:99|999:1010.

Valid Values—Enter ranges of valid values as described in Decimal above.

Editable Valid Values—Check to enable editing of default or entered integer.

Long

Default Value—Enter a default long.

Constraints—Enter a range of acceptable numbers separated by a colon. You can also include several numbers or ranges separated by the pipe (|) character. If you specify a range, the lowest number must be to the left of the highest number. For example 9:99|999:1010.

Valid Values—Enter ranges of valid values as described in Decimal above.

Inventory Reference

Select the *Reference Type* entity with the list that appears when you click the green plus (+), then use the side-by-side widget's arrows to move available attributes from *Available* to *Selected*. You can change the *Reference Type* by deleting it with the red minus (-), then selecting a new type with the green plus.

String

Default String—Enter a default string.

Valid Values—Enter valid values as described in Coded Value above.

Editable Valid Values—Check to enable editing valid values.

Constraint—Enter the regular expression constraints, if any, on the string attribute.

Constraint Description—Enter the message to appear if the regular expression constraints are not met.

Min / Max Length—Enter the minimum / maximum number of characters in a valid string.

Click *Apply* to accept your edits for the attribute, or *Cancel* to abandon them.

Use an existing Parameter Schema for this Adaptive CLI

Select this, and a *Select Existing* button appears. Clicking this button opens a selector where you can select from previously-configured attribute schemas (collections of attributes) to use in the Adaptive CLI you are configuring.

Validating IP Address Variables

Programatically, IP address attributes support four extended properties: IP_MASK, SUBNET, ALLOW_32_BIT_MASK, and ALLOW_ANY_VALID_IP. The state of the first two largely defines OpenManage Network Manager's responses.

IP_MASK—Determines whether OpenManage Network Manager accepts an IP address OR a subnet/subnet mask. The value accepted is an IP address attribute when false, subnet/subnet mask when true.

SUBNET—This property determines whether a subnet value must be provided or not, and controls display of the subnet portion of the widget. Valid subnet values are 1-31.

By default, when both of the above are false, the attribute only accepts valid IPv4 addresses. For example: 10.10.10.4

If IP_MASK is false and SUBNET is true then OpenManage Network Manager accepts any valid IP address with a subnet specified. The address must be an IP within the specified subnet. For example, 10.10.10.4/24 is a valid entry whereas 10.10.10.0/24 is invalid since it represents the subnet id, not an actual address within the subnet.

If IP_MASK is true and SUBNET is false, then OpenManage Network Manager accepts one of the 32 valid subnet masks. The widget displays pick list for user to choose from. For example 255.255.255.0

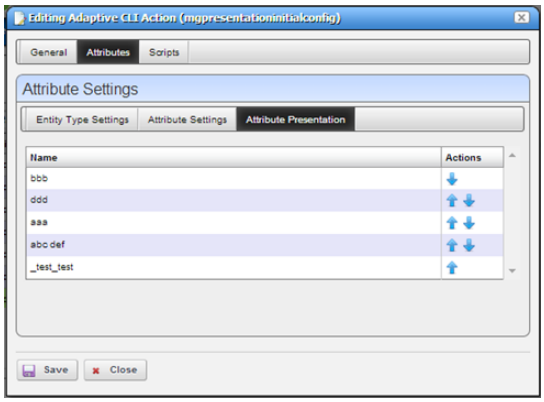
If IP_MASK is true and SUBNET is true, then OpenManage Network Manager accepts a subnet id (the first IP address within a subnet). For example 10.10.10.0/24, with 10.10.10.0 as the first address within the subnet spanning 10.10.10.0 to 10.10.10.254. Entering an IP address within the subnet, say 10.10.10.4/24, the attribute would convert that to 10.10.10.0/24

ALLOW_32_BIT_MASK—Valid subnet values are between 1 and 31. To extend this to support a 32-bit subnet, which is essentially a single IP address (10.10.10.4/32), set the ALLOW_32_BIT_MASK property.

ALLOW_ANY_VALID_IP—To accept either an IP address, IP address and subnet or subnet, then IP_MASK remains false, SUBNET is true. With the ALLOW_ANY_VALID_IP true, the subnet field is optional and OpenManage Network Manager disables any requirement that a subnet id be specified. Basically the only validation is that a valid IP address is entered. For example, in this configuration, 10.10.10.4, 10.10.10.4/24 and 10.10.10.0/24 would all be valid.

Attribute Presentation

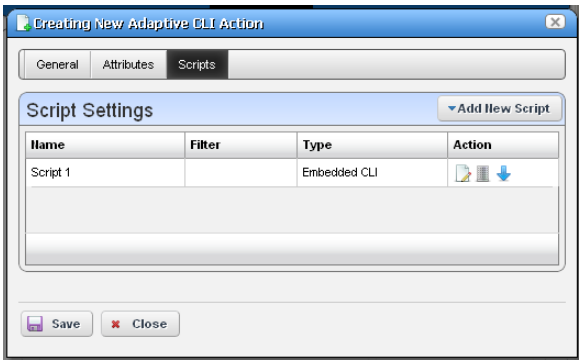
This panel lets you reorder attributes by selecting an attribute, then clicking the up/down arrows. Exporting or importing a reordered Action preserves the configured order of attributes.



If you change the attribute order after scheduling the Action, it does not affect the execution of the scheduled Action. If you use the same Entity Type (schema) for another Action attributes appear in the same order.

Scripts

This screen manages the Adaptive CLI scripts created to query (show) devices or configure them. OpenManage Network Manager runs only one script per target.

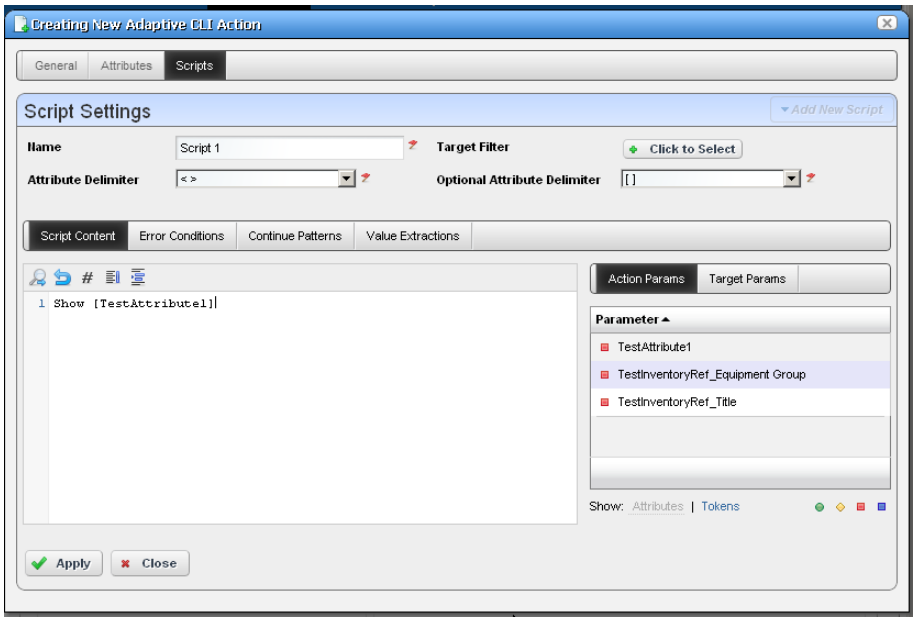


Notice you can order multiple scripts with the arrow(s) to the right of a listed script. Only one schema of attributes exists for each Adaptive CLI, so the same attribute(s) appear when you construct each script.

OpenManage Network Manager uses the script's filter to match the target. For example, imagine two scripts for which the first has filter = target.type = SWITCH, and the second has no filter. Then only SWITCH devices run the first script and quit. All remaining targeted devices do not run first script. Instead they run the second script since that script has no filter. Only one script runs on the selected target equipment. The ordering lets you to make the most efficient use of that one-run-per-target pattern.

Script Settings

Click *Add New Script* to create a new item in those listed at the top of this screen, or select and item and click the *Edit* icon to its right to alter it. When you create a new script, you must select either *Embedded CLI* or *Perl*. Embedded CLI scripts are command-line interface (CLI) interactions. See Perl Scripts on page 291 for more about using Perl.



Clicking the *Delete* icon removes a selected item. Notice that the up/down buttons to the right of the list allow you to re-order selected items (they run from top first to bottom last).

See Attribute Appearance and Validation for a description of what constitutes a valid attribute.

NOTE:

You must mark an attribute as required before adding it to the script. If you add an attribute before you mark it as required, you must remove it from the script, mark it as required, then re-add it. In some browsers, after adding the attributes you must click in the script screen to ensure that the changes persist.

Name—Enter an identifier for the script you are creating or altering.

Target Filter—Click the plus (+) to create a filter that describes the target for this script. For example, this filter could confine the action of the configured script to devices from a certain vendor, or only devices with an operating system version later than a certain number. Since you can have several scripts, those Adaptive CLIs with a single label ("Show Users," for example) could therefore contain several scripts with syntax appropriate to a variety of devices and operating systems.

CAUTION:

Adaptive CLI supports only filters that select the Managed Equipment type of device.

Attribute Delimiter—The delimiter(s) you select from the pick list here surround the attributes you designate as mandatory. See Adaptive CLI Script Language Syntax on page 290 for more about these.

Optional Attribute Delimiter—The delimiter(s) you select from the pick list here surround the attributes you designate as optional. See Adaptive CLI Script Language Syntax on page 290 for more about these.

All but *Delete* open a script editor with the following panels:

- Script Content
- Error Conditions
- Continue Pattern
- Prerequisite Validation
- Value Extraction

Script Content

On the left, you can enter text, *Search* by clicking the magnifying glass, and use *Cut*, *Copy*, *Paste*, *Undo*, *Jump to Line #*, *reformat*. The *Attributes* appear under *Target Params* on the right of this text entry screen. Double-click an attribute to insert it unless you are writing a Perl script; this feature does not work for Perl. Right-click the previously-configured attributes in this panel to designate them as *Mandatory*, *Optional*, *Not Applicable* or *Non Configuration* in a context menu that appears when you right-click.

NOTICE

OpenManage Network Manager does not send *Non Configuration* attributes to the device with the script. These are comments that can serve to remind users of critical information. For example, you can make *Non Configuration boolean attributes into a checklist for someone executing a script, and the history of this script can record whether* OpenManage Network Manager *made these checks when the script ran.*

Notice that the *Search* also permits Regular expressions.

You can also enter two types of script language here. See Adaptive CLI Script Language Syntax on page 290 for a description of the internal *If* capabilities. If you need more elaborate scripting, you can also use Perl scripts to send text to devices. See *Perl Scripts* on page 291 for a description of those capabilities.

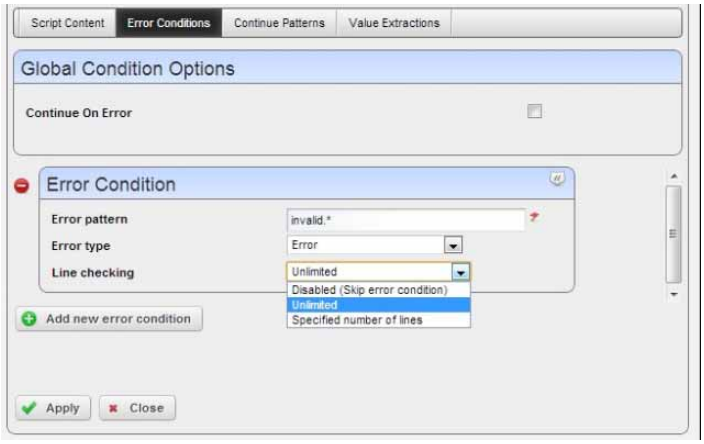
Click *Apply* to accept the script you have configured.

NOTE:

Some versions of Firefox do not save attributes when you click Apply. **Workaround:** When you have added the new attribute into the script content click the cursor back into the script content, then click Apply.

Error Conditions

The error condition lets you configure errors for your script.



Check *Continue on Error* under the Global Condition Options, if you want the script to not stop when it encounters an error. Click *Add new error conditions* to configure a condition at the bottom of this screen with the following fields:

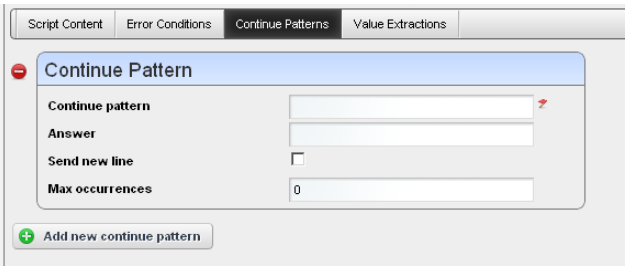
Error Pattern—Enter a regular expression for the error. You can also click the icon in the upper right corner to test the expression. See Regular Expression Testing on page 306.

Error Type—Select from the pick list of options (*Error, Warning, Ignore*).

Line checking—Select from the pick list (*Unlimited, Disabled (Skip error condition), Specific number of lines*). If you select a specific number of lines, enter the number of lines of the script output to check for the pattern specified, after each command execution. An error message is most likely to appear immediately right after the command is invoked.

Continue Pattern

Like Error Conditions, this screen lets you enter conditions to which script execution can respond.



The Continue Pattern editor operates like the Error Conditions editor, but has slightly different fields.

Continue Pattern—If you expect the device output of a script to prompt to continue, you may add a *Continue Pattern* with a regular expression to parse. You can also click the icon in the upper right corner to test the expression. See Regular Expression Testing on page 306.

Answer—This field specifies the *Answer* to the *Continue Pattern* prompt.

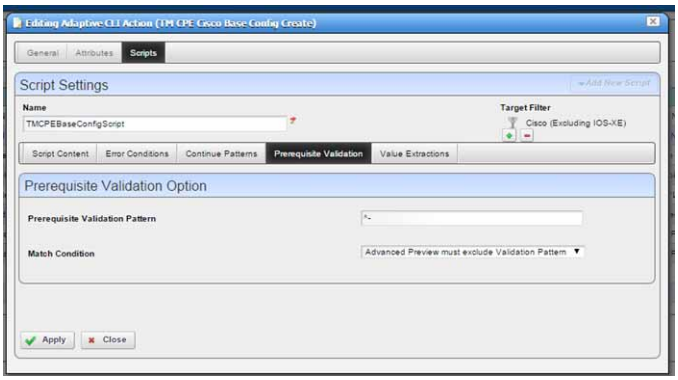
Send New Line—For some devices, a single key response without a new line would be sufficient; in such cases, you may need to uncheck the *Send New Line* option.

Max Occurrences—Indicates the maximum number of times respond to a prompt. The default value zero (0) indicates no limit.

Prerequisite Validation

Some devices (JUNOS and Cisco XR) allow you to preview the result of an Adaptive CLI before actually executing it on devices that support such an advanced preview. Standard preview simply discloses what OpenManage Network Manager sends to devices; advanced preview requires a device response indicating the effect.

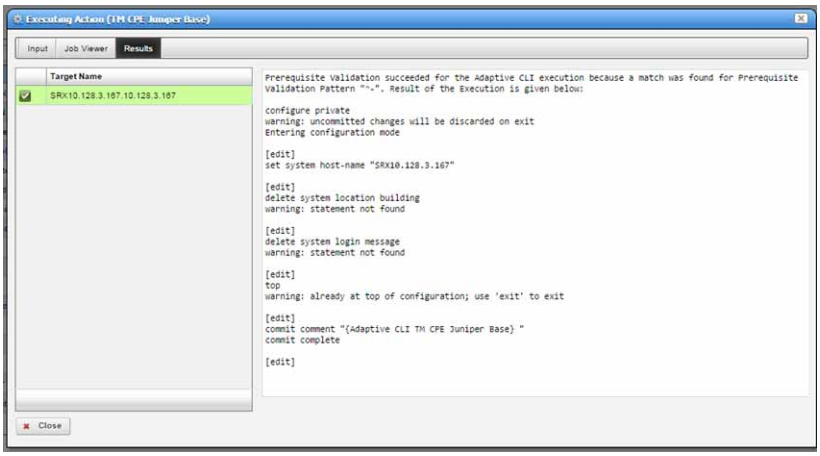
A *Prerequisite Validation* tab appears for an Show or CLI Configure Command Adaptive CLIs that lets you allow or prevent Adaptive CLI execution based on a regular expression match during such advanced previews.



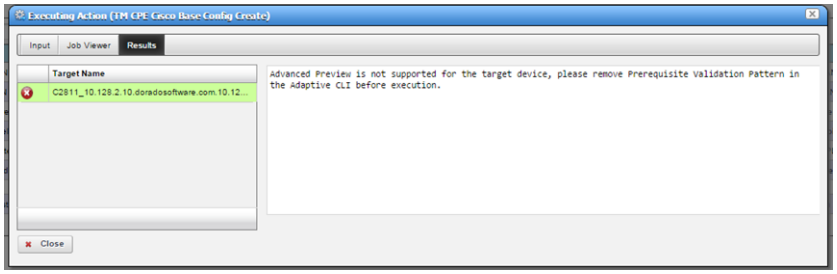
This tab provides options to select the following.

Prerequisite Validation Pattern—This is a regular expression that is a condition to prevent execution of the Adaptive CLI.

Match Condition—For a supported device, Match Condition lets you select whether execution should be prevented if a match occurs for the Prerequisite Validation Pattern on any line of the Advanced Preview Results obtained from the device. Alternatively you may prevent execution if a match does not occur for any line of the advanced preview Result.



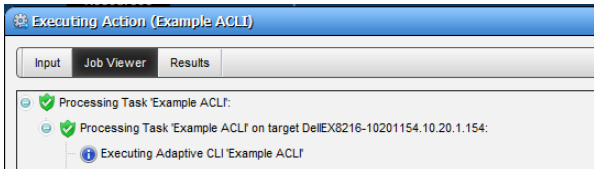
For non-supported devices, if you provide a Prerequisite Validation Pattern, on execution you are advised to edit the Adaptive CLI and remove the pattern before execution.



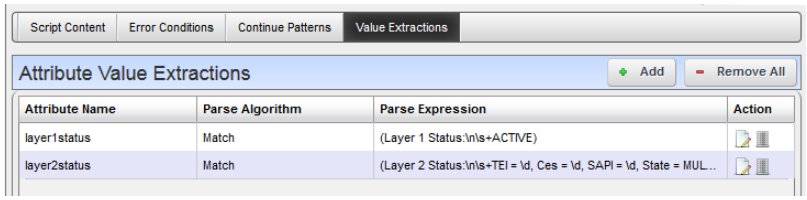
Prerequisite Validation does not appear for types other than CLI Show Command and CLI Configure Command.

Value Extraction

To support Adaptive Service and Active Monitor functions, Adaptive CLI provides a way for the user to define output schema attributes. This tab is active only if you have configured schema attributes to store values previously in the Attributes portion of this editor.



This lets you *Add*, *Edit* or *Delete* extracted attributes, like Error Conditions's editor. To clarify configured *Attributes*, *Parse Algorithms*, and *Parse Expressions* accompany scripts, they appear in a table. Use the *Add* button to create more Value Extractions, and the *Edit* or *Delete* buttons to the right of listed patterns to alter or remove them.



Configure Value Extractions with the following fields:

Attribute Name—This field specifies the name of the extracted attribute. To specify the output value of an attribute, select it from the provided list.

Attribute Type—The data type of the attribute extracted. Only schema attributes of simple type String, Integer, Long, Float, Double, and Boolean are available to choose from.

Parse Algorithm—Select from the pick list (*Extract*, *Match*). For match algorithm, the result is either *true* or *false* for the Boolean attribute type, 0 or 1 for numeric types, or "*true*" or "*false*" for String type.

NOTE:

Currently, Active Performance Monitor supports only numeric types, but you can configure extraction to produce numbers. See Example 5: Monitor Text Values on page 303 for an example.

Parse Expression—Enter a regular expression for Parse Expression and the Parse Algorithm (Extract or Match) used when evaluating the device output on a given script execution. OpenManage Network Manager matches the regular expression for sub-strings, so no need to provide a leading and trailing "match all" regular expression. (.*).

See Regular Expressions on page 333 for more information about what is these expressions can do. You can also click the icon in the upper right corner to test the expression. See Regular Expression Testing on page 306.

Click *Apply* to accept your edits, or *Cancel* to abandon them. Click *Add new attribute extraction* to add more such patterns to your script.

Attribute Appearance and Validation

Invalid schema attribute names appear in the script in red italics. This indicates that you cannot use such attributes in the script.

Valid attribute names contain alphanumeric characters and underscore (_). They must begin with either an underscore or a letter [A-Za-z].

All blank space characters in the schema attribute name are converted to underscore (_) by default.

A schema attribute name that is invalid in Adaptive CLI may still be valid in other entities, so you can specify them in the schema but they are not usable by Adaptive CLI.

External Executable

External executable Adaptive CLIs essentially run external scripts from the OpenManage Network Manager environment. For example, you could run the DOS `dir` command (and schedule its execution). Make sure you select External Command as the Type of Adaptive CLI in the editor when you create an Adaptive CLI that refers to an external command. Also, make sure the `Net::Telnet` package is installed with Perl.

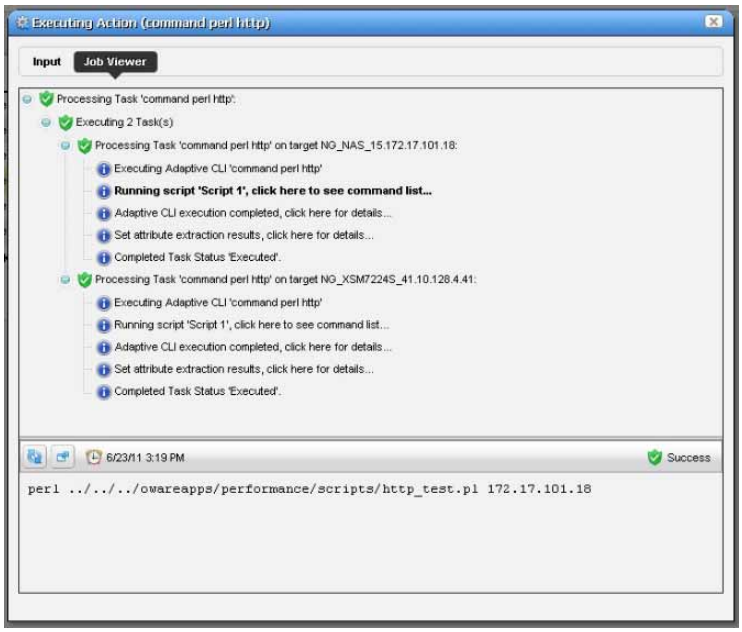
NOTE:

To run targetless external commands In a distributed environment, you must add the current application server's IP address to a mediation partition's routing entry. The external command runs at one of mediation servers that belongs to that mediation partition. Any external scripts must exist on all mediation servers within that mediation partition, and the directory path must be the same. Best practice is to use a shared network drive (or cloud) whenever you need to access files from multiple servers.

You can execute external commands with a device as target, using device attributes as input parameters to the Adaptive CLI script. See some of the Seeded External Scripts on page 287.

Audit Trail

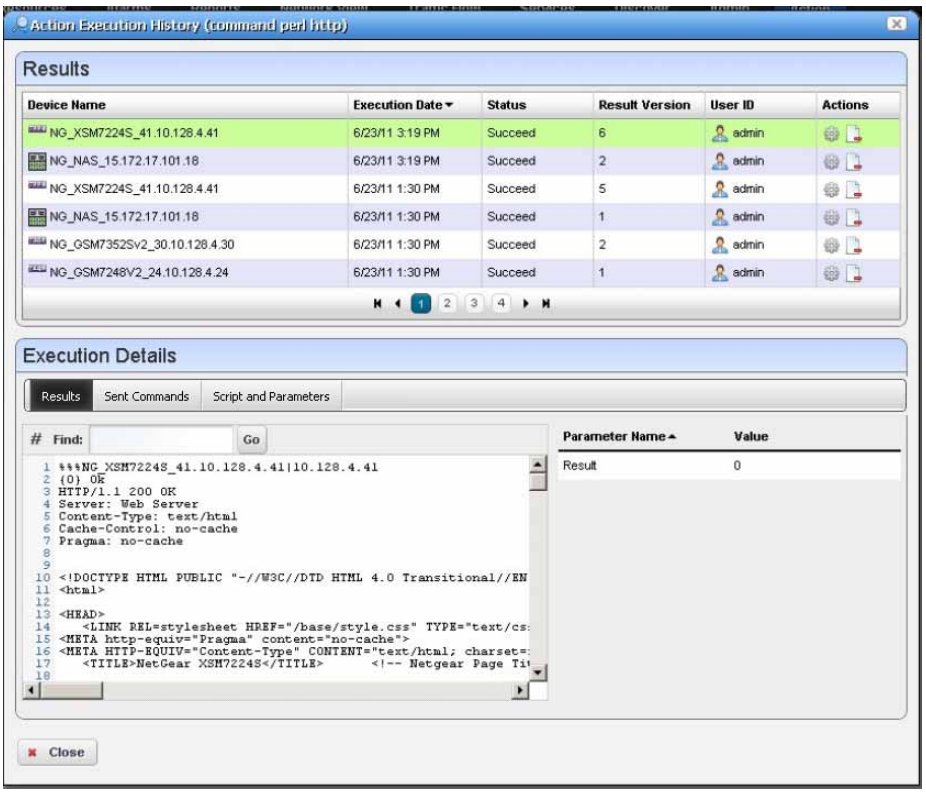
When you execute a script, the audit screen displays information about it.



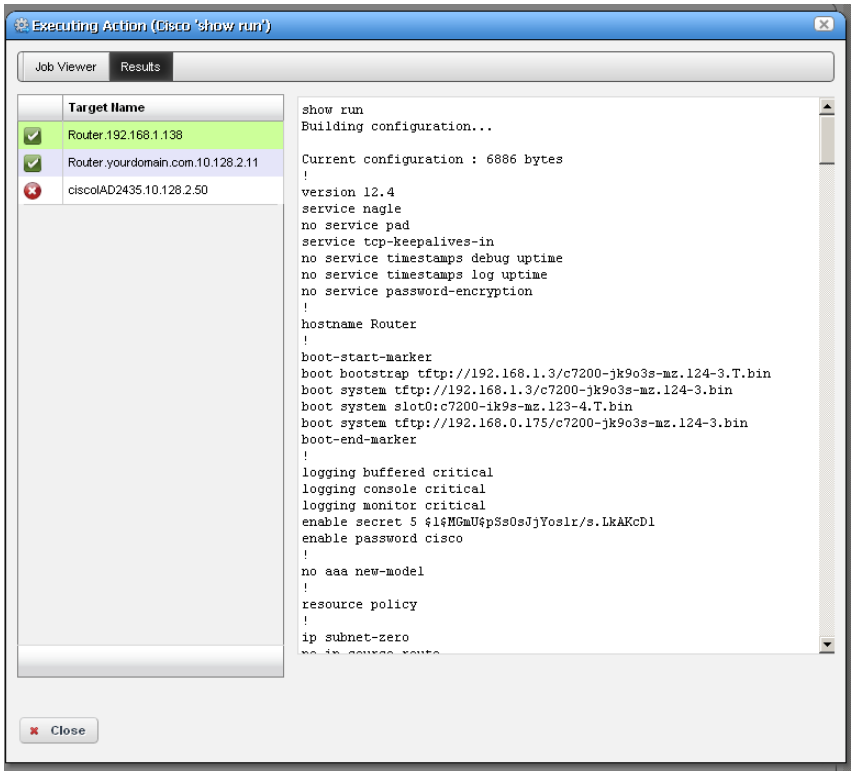
By default, this screen often conceals the *info* circles in this screen. To see them, click the icon next to the refresh icon to open the message level selector and check the *info* circle level of reporting, then click *Refresh* to see those blue circles.

Results

OpenManage Network Manager stores the results of running a script as lines the Execution Details snap panel. Right click the particular command run in the snap panel at the bottom of the Expanded Actions Portlet. Tabs show the Results, Sent Command, and Script and Parameters. When viewing a script run the results of running it appear target device-by-device.



Results can also appear in the audit screen messages and in the *Results* panel of the *Action* job viewer screen.



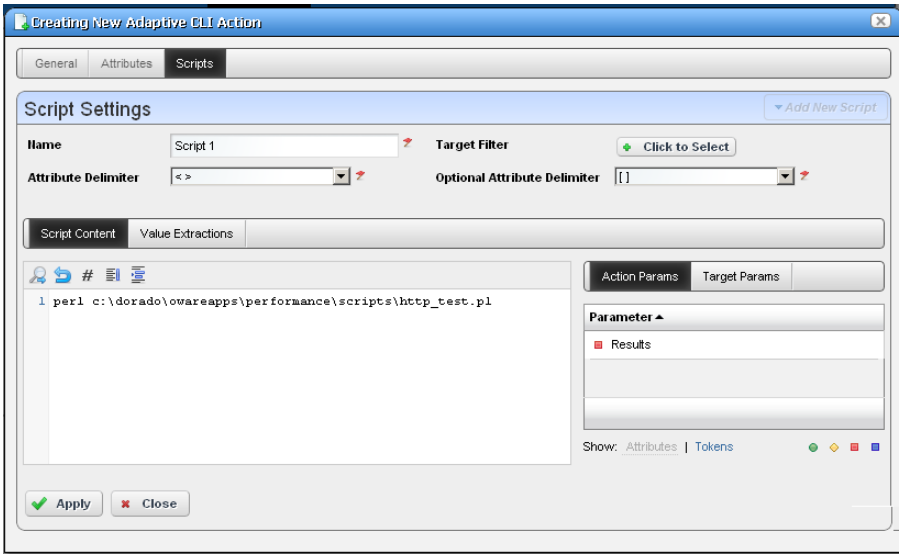
You can also extract parameters for these external commands as is described in Value Extraction on page 283.

Seeded External Scripts

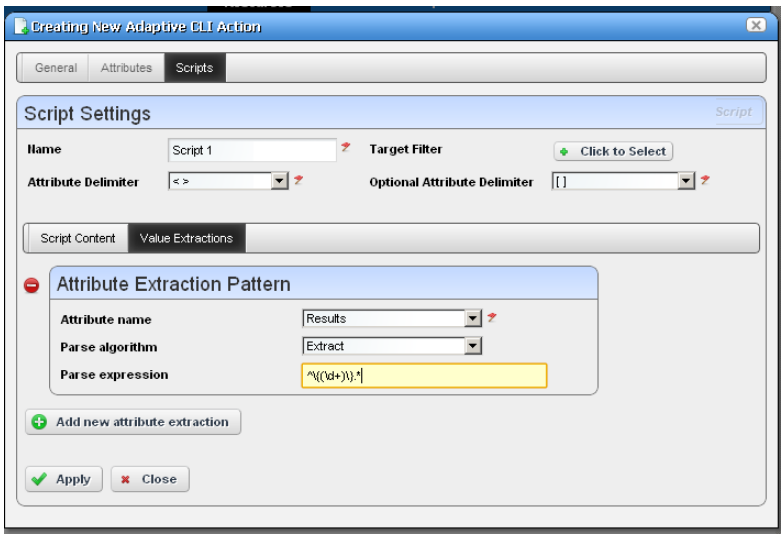
Several external perl scripts come with OpenManage Network Manager as examples of the kind of commands you can execute (and Monitor, see Adaptive CLI on page 196 in Performance Monitoring). These are in `\owareapps\performance\scripts` under the installation root.

To run these, the scripts panel in the Adaptive CLI editor should contain something like the following:

```
perl ../../../owareapps/performance/scripts/http_test.pl
```



Notice that these also include a parameter (*Result*) that contains values extracted.



Set up attribute extraction in the *Values Extraction* tab of the script editor.

Script Names and Functions

Linux installations must have the Net::Telnet package installed with Perl.

common.pl—Common functions defined for scripts in this directory.

dns_test.pl—Check if DNS can resolve the specified host name.

finger_test.pl—Check if the finger service is running on a specified host.

ftp_test.pl—Check the FTP service is running on a specified host.

http_test.pl—Check the HTTP service is running on a specified host.

nntp_test.pl—Check if the NNTP service is running on a specified host. (Public NNTP server to test: news.aioe.org)

peping_test.pl—Check if a target is pingable from the specified remote host.

pop3_test.pl—Check if the POP3 service is running on a specified host.

smtp_test.pl—Check if the SMTP service is running on a specified host.

telnet_test.pl—Check if the TELNET service is running on a specified host.

See Create a Monitor for an External Script on page 192 for more specifics about monitoring these.

If you have a clustered installation, then every server in the cluster must have scripts installed to the paths Adaptive CLIs using them specify.



How To:

Make an Adaptive CLI Run an External Script

The following demonstrates Adaptive CLI running an example Windows external batch file (script) that includes command line parameters. Follow these steps to create this training example:

1. Right click in the *Actions* portlet to create a new Adaptive CLI.
2. In the editor's *General* tab, enter a name (here: Test HelloWorld.bat), and select *External Command* as the type.
3. Click the *Attributes* tab, and create Hello World Schema with two string attributes (in the *Attribute Settings* sub-tab). Here, we make *Command1* and *Command2*.
4. In the *Script* tab, make the Hello World Batch File command (the example name), whose contents are:

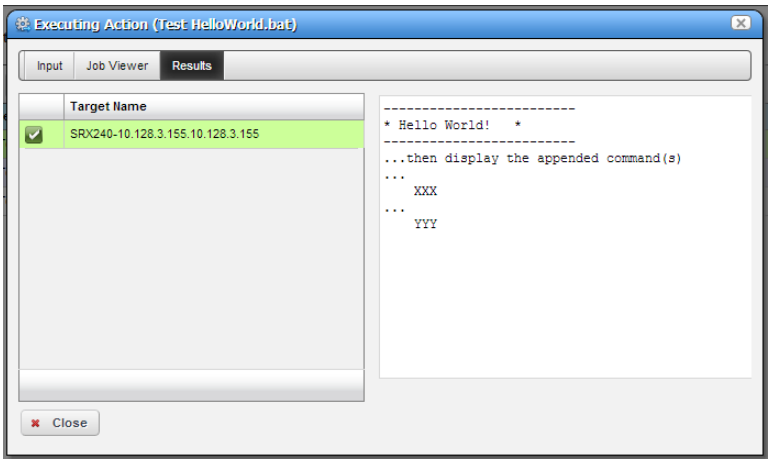
   ```
   c:\HelloWorld.bat [Command1] [Command2]
   ```

   Both command line parameters are optional in this example, but you can create such scripts where parameters are required before the script will run. Select a parameter and click the Tokens at the bottom of the screen to arrange that.
5. After you have finished configuring the script, click *Apply* and *Save*.
6. Before running this Adaptive CLI example, you must create a batch file called `c:\HelloWorld.bat`. Here are its contents:

   ```
   @ECHO OFF
   ECHO -------------------------
   ECHO * Hello World!   *
   ECHO -------------------------
   ECHO ...then display the appended command(s)
   ECHO ...
   ECHO     %1
   ECHO ...
   ECHO     %2
   ```
7. After creating and saving `c:\HelloWorld.bat`, right click Test HelloWorld.bat in the Actions portlet, and select *Execute*.
8. You must select a target device before going further, even though this script does not require one. Select any device.
9. A screen offering to let you specify Command1 and Command2 appears. For the sake of this example, any string you enter works. We'll enter XXX and YYY.
10. Click the *Execute* button.

11 The Job Viewer screen appears displaying the command line you have specified (`c:\HelloWorld.bat XXX YYY`) in informational messages. You typically have to configure the Job Viewer so these appear. They are concealed by default.

12 Finally, the *Results* screen appears with the device you specified on the left, and the result of the batch file run on the right.



For further practice, try running a script of your own, or one of the seeded Perl Scripts (see Seeded External Scripts on page 287).

Adaptive CLI Script Language Syntax

The following is the Adaptive CLI scripting language syntax:

- CLI script is a line-based syntax. In other words, each line's syntax has to be completed.
- CLI script supports primarily two features: Attributes and Conditional Blocks.

Attributes

Each attribute in the script is marked by a delimiter. The following delimiters are supported:

```
<>  []  {}  ()  $  %  @  #
```

Think of Attribute delimiters as a pair of open/close markers surrounding a variable name. For single character Attribute delimiters, there is no closing marker (the close marker is empty).

Examples of Attributes are:

```
<var>, [var], {var}, (var), $var, %var, #var, @var
```

The default mandatory delimiters are <>, and the default optional delimiters are `[]`, but you can change those default settings. That means an Attribute variable like <var> may represent a mandatory or an optional Attribute depending on what are set as delimiters.

NOTE:

Single delimiter symbols require a space after the attribute. These do allow values immediately before the symbol. Perl requires a space after the attribute, or the attribute's closing delimiter, but values immediately before single delimiters works.

Here is an example of a command line with a mandatory and optional Attribute:

```
show <mandatory> [optional]
```

If you set the `<mandatory>` Attribute to *interface* and do not set the `[optional]` one, then the resulting command would be this:

```
show interface
```

If you set the `<mandatory>` Attribute to *interface* and set `[optional]` to *brief* then the resulting command would be:

```
show interface brief
```

Conditional Blocks

Every line in the script is presumably a command to be sent to the device, except for lines that denote either a beginning or ending of a conditional block.

The begin conditional block marker is tied to a Attribute and has the following syntax:

```
<optional-open-delimiter> IF optional-attribute <optional-close-delimiter>
```

The end conditional block marker has the following syntax:

```
<optional-open-delimiter> ENDIF optional-text < optional-close-delimiter>
```

Here is an example of a conditional block, where the Attribute delimiters are <>, optional delimiter is `[]`, and the conditional Attribute variable is `set`:

```
[IF set]
  execute this command
  and execute this command
[ENDIF set]
```

If the Attribute set has a value then the block is evaluated; otherwise, it is ignored. The text after `ENDIF`, that is `set` or whatever is not required and it is ignored.

Nested conditional blocks are allowed.

Perl Scripts

This section describes the details of using Perl scripts within Adaptive CLI. See Using Perl in Adaptive CLI on page 264 for more about why to use Perl.

The Perl output goes to the selected target device. Typically, this means creating lines like the following:

```
println("show $param");
```

or

```
print("show $param\n");
```

You must specify parameters within the script (like `$param`) in the screen described in Attributes on page 272. Unlike its internal scripts, Adaptive CLI does not automatically create attributes. You must also manually configure created attributes to be *Mandatory*, or *Optional* in that screen.

A few things to remember when using Perl:

- The normal output of your Perl scripts (to stdout) are the commands sent to a device by this application.
- If your script produces an error message (to stderr), the job fails with that message and all script outputs are ignored. You can validate a script before sending any command to the device by using die(...) and warn(...) functions in Perl to produce error messages to stderr. Such messages trigger the script's failure.
- For such scripts to operate correctly, you must have Perl installed on the directory path for all OpenManage Network Manager servers.

- Perl may not come with OpenManage Network Manager and must be on the server system for it to work with Adaptive CLI.
- You can install your version of Perl and set the PATH environment variable accordingly so that one can run `perl -v` from the command line (where the OpenManage Network Manager server is to be started). Adaptive CLI invokes that same `perl` command.

  If for some reason Adaptive CLI, fails to invoke the default `perl` command, it reads the setting of `activeconfig.perl.exe=...` inside `owareapps/activeconfig/lib/ac.properties`, and uses that alternative command.

  Note that the default `activeconfig.perl.prefix=` setting in `ac.properties` is prepended to every Perl script. It basically forces the script to `use strict` mode and provides a convenient `println` method for the user. Knowledgeable Perl users can change this default behavior setting but should be careful about it. Remember, best practice is to override properties as described in Overriding Properties on page 71.

- The standard output (using `println`) of the Adaptive CLI Perl script represents the command set that is to be sent to the device. For convenience, a `println` subroutine is embedded with the script.
- Adaptive CLI with Perl scripts must contain valid Perl under the "strict" pragma (`use strict;`). If you import or migrate from a previous version a Perl script that does not pass this "strict" criterion, you must rewrite it for "strict" compliance before it can be successfully edited or copied.

NOTE:

When you import a Perl Adaptive CLI that doesn't pass strict, you can execute it without problems. However, you *cannot* edit it at all, unless you first edit it to pass strict (or it won't even let you save the changes).

The following Perl Example may be of interest.

Perl Example

The following is an example Perl script for Adaptive CLI:

```
#
# A script example for testing against a Cisco-XR machine.
#

# The following variables (attributes) are defined in the schema,
# and their values are assigned when the script
# is invoked from the Adaptive CLI (or Resources) manager.
# These variables will be declared with values and prepended
# to each script automatically.  Something like:
#
# my $FromPort=<some number>;
# my $ToPort=<some number>;
# my $Mtu=<some number>;
# my $Desc=<some text>;
#

print("config t\n");

foreach ($FromPort .. $ToPort) {
```

```
  my $Desc = "$Desc Port #$_";
  my $addr = 100 + $_;

  print("interface GigabitEthernet0/1/1/1.$_\n");
  print("description $Desc\n");
  print("ipv4 address 10.10.100.$addr 255.255.255.0\n");
  print("ipv4 unreachables disable\n");
  print("mtu $Mtu\n");
}

print("exit\ncommit\nexit\n");
```



How To:
Create Adaptive CLI Examples

The examples that follow may not work for your device. They are often created with a specific device, with specific syntax. Best practice is to telnet to the device you plan to target with your Adaptive CLI, and test the command line there first. Then configure any extraction you plan to use based on that testing.

The following describes the basics of creating and using Adaptive CLIs.

Example 1 - Existing Show Run uses an existing, seeded Adaptive CLI to show protocols.

Example 2 - New Adaptive CLI describes making and using a new Adaptive CLI.

Example 3 - Adaptive CLI with Reboot shows you how to make an Adaptive CLI that requires rebooting the target device(s).

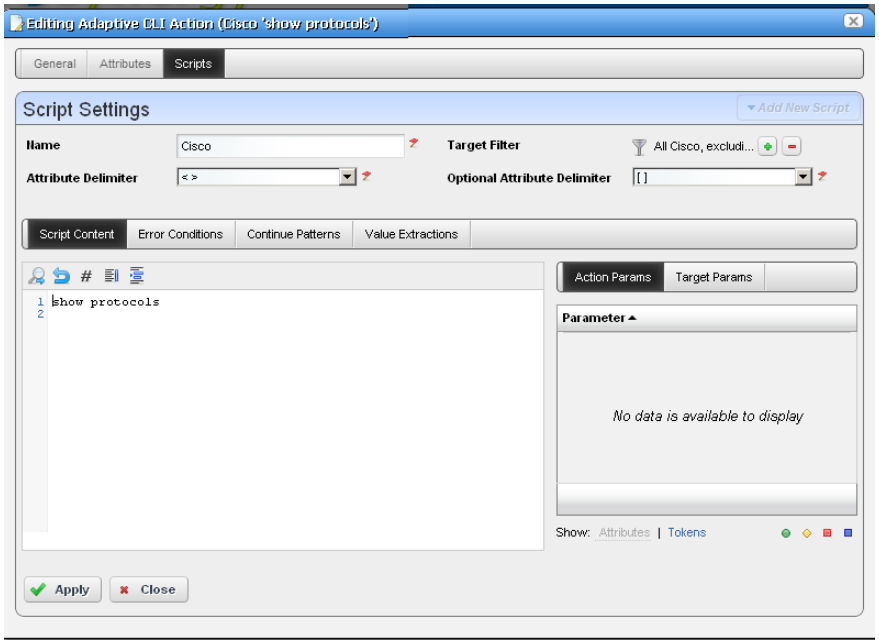
Example 4 - Adaptive CLI To Extract Upload / Download Speeds demonstrates Adaptive CLI that extracts information from the target device, then displays the results on a dashboard.

Example 5: Monitor Text Values demonstrates using and Adaptive CLI configured to monitor attributes with strings that indicate their status.

Some devices do not respond to commands unless they are in the correct state. For example, some Dell devices must not be in “Simple” mode to respond to Adaptive CLIs. Take account of this as you create Adaptive CLIs.

Example 1 - Existing Show Run

1 Adaptive CLI Manager has pre-seeded tasks and diagnostic commands based upon the drivers you have installed. For example: the *Cisco* '*show protocols*' command. Right-click and Select *Edit* to view and / or alter this Adaptive CLI.

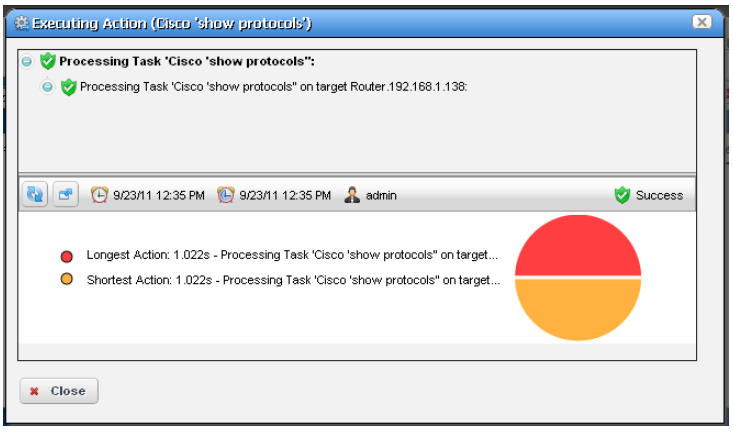


2 Click the *Edit* icon next to the Cisco script. The *Scripts* tab in this editor appears above, displaying the `show protocols` command to be sent target devices. Notice (in the upper right corner) that this Adaptive CLI filters so it applies to all Cisco devices excluding PIX.

3 Close the editor(s), and select this Adaptive CLI.

4 Right click to *Execute*, and select the target equipment for this run in the next screen. The screen that appears is a standard OpenManage Network Manager equipment selector. The Adaptive CLI is valid only on devices that pass the Target Filter mentioned in step 2, but the selection here narrows the target devices for the Adaptive CLI.

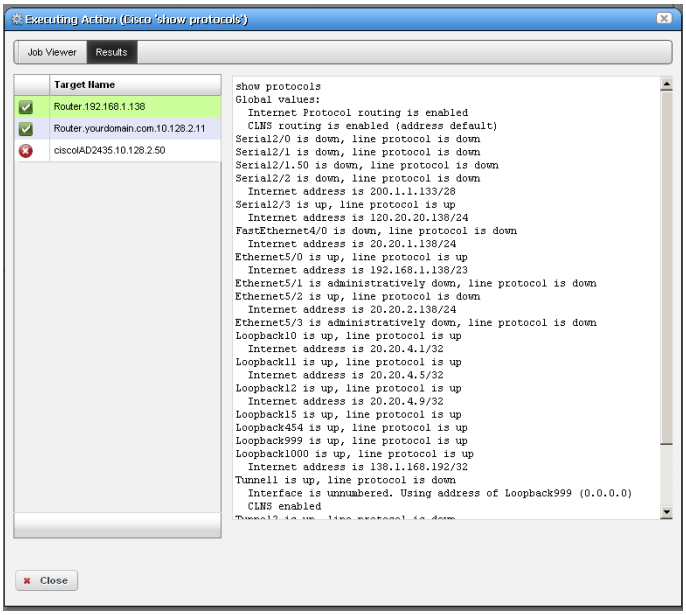
5 An Audit trail screen tracks the execution progress



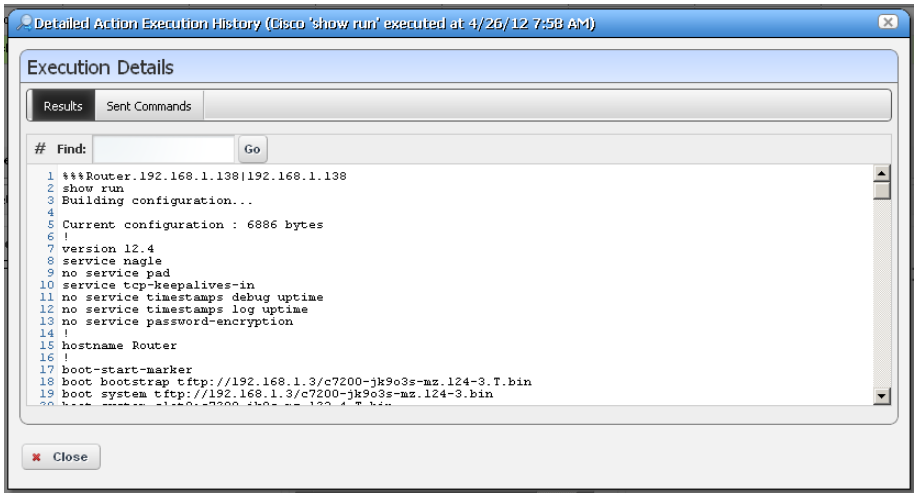
6 Select the Adaptive CLI you ran in the Expanded Portal, and right-click the execution run that appears in the *Execution History* snap panel at the bottom of the screen.

7 Right-click and select *Execution Details*.

8 View latest results classified by the device you select on the left.



9 View latest results by right-clicking in the *Execution History* snap-in of the expanded Action portlet. You can use the *Find* search box to find matches to strings within the results.



Click *Go* to see the next match.

10 You can also look in the *Sent Commands* tab to see what actually went to the device.

Example 2 - New Adaptive CLI

1 Create a new Adaptive CLI. Right-click and select *New*.

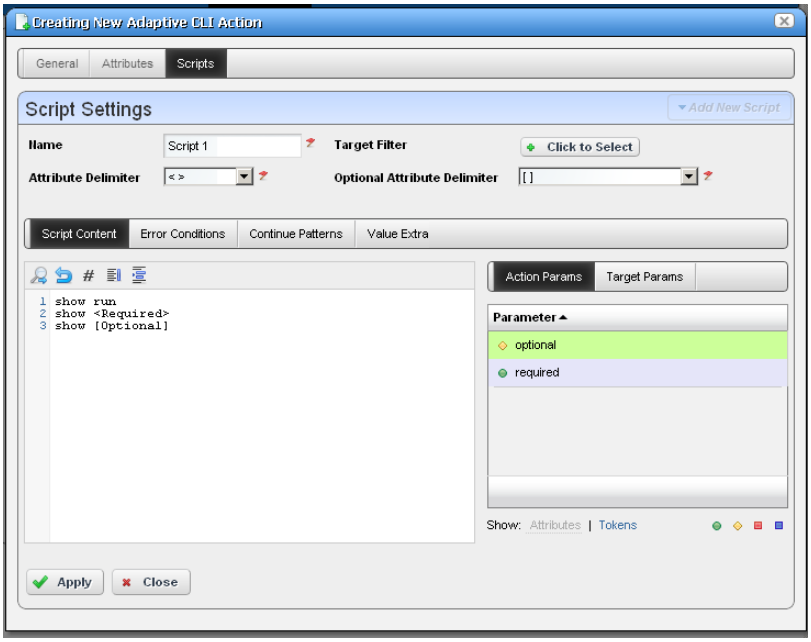
2 Name this (for example "Test ACLI")

3 In the *Attributes* panel, create string attributes named *required* and *optional* after creating a new Parameter Schema (for example “test123”).

4 In the *Script* panel define the Attribute Delimiter (< >) and Optional Attributes Delimiter ([ ]) and enter the following three scripts:

```
show run
show <required>
show [optional]
```

Notice that the created attributes appear in the panel on the right of this screen.



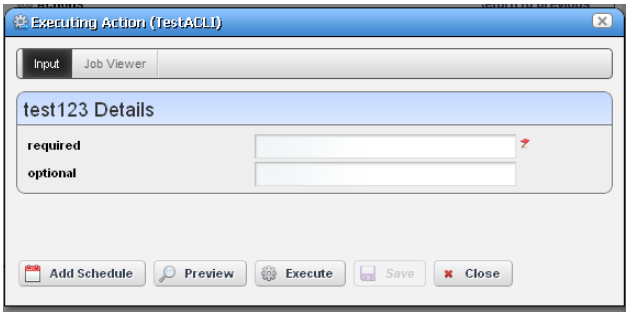
5 Select the attribute “required,” then click the *Required* icon (the green circle) in the lower right corner to of this screen to associate this icon with the Required attribute. Similarly, associate the *Optional* icon with the attribute “optional.”

Notice that you can double-click the attributes listed in the panel on the right, and they appear in the script editor at the cursor.

6 Save this Adaptive CLI

7 Execute it with *action* > *Execute*.

8 Notice that the attributes entered now are visible as inputs.



When you enter values for these, they accompany the `show run` sent to the target devices. Notice that you *must* enter the required variable, or execution fails.

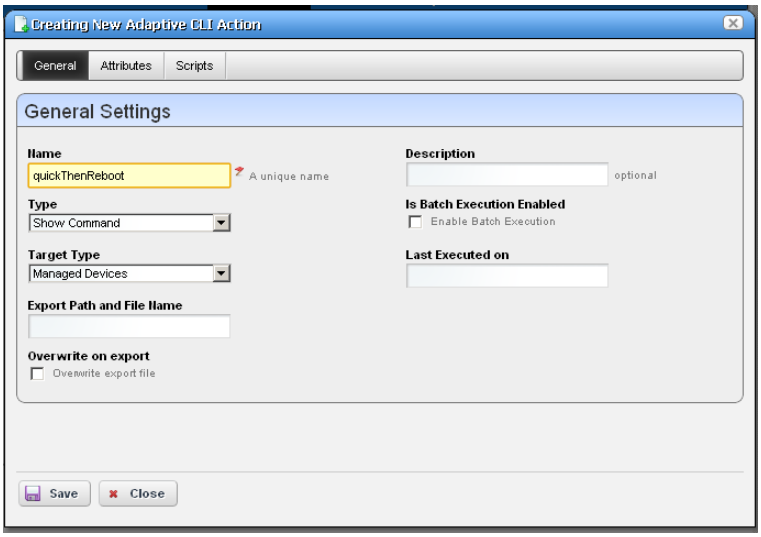
9 Select a target.

10 Click *Execute*. The `show run`, and any other required / optional run commands' results appear. These are searchable with the results screen.

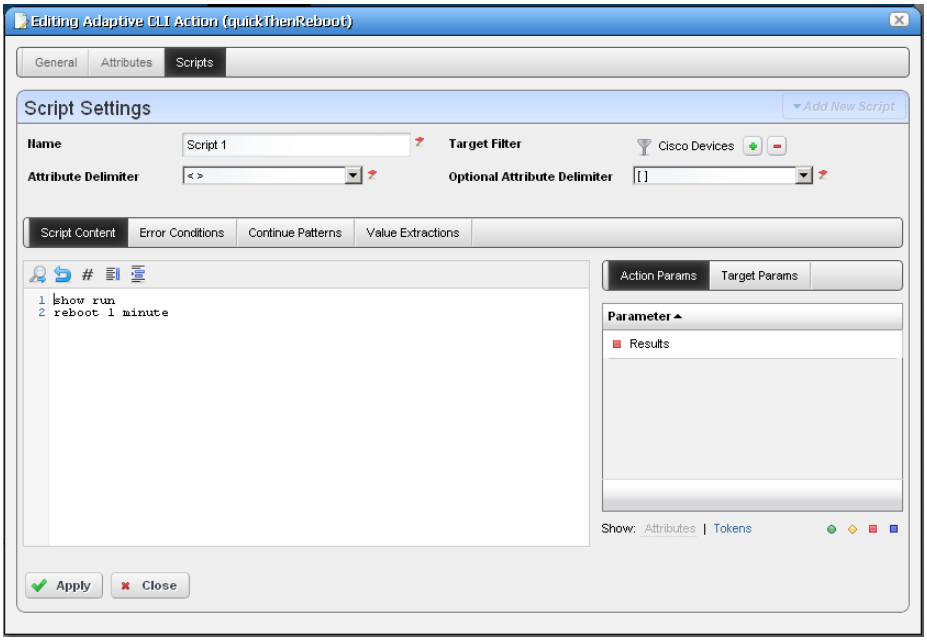
Example 3 - Adaptive CLI with Reboot

The following describes how to set up multi-line ACLI with error / success tracking for a command sequence that requires reboot.

1 Create an example configure Adaptive CLI command (here *quickThenReboot*).



2 Separate commands into parts. First issue the command (here `show run`), then issue the reboot command with a parameter that allows a prompt return before actual reboot (a delay, for instance). If the first command fails the ACLI doesn't continue, so that makes using the reboot command second the solution.



In our example:

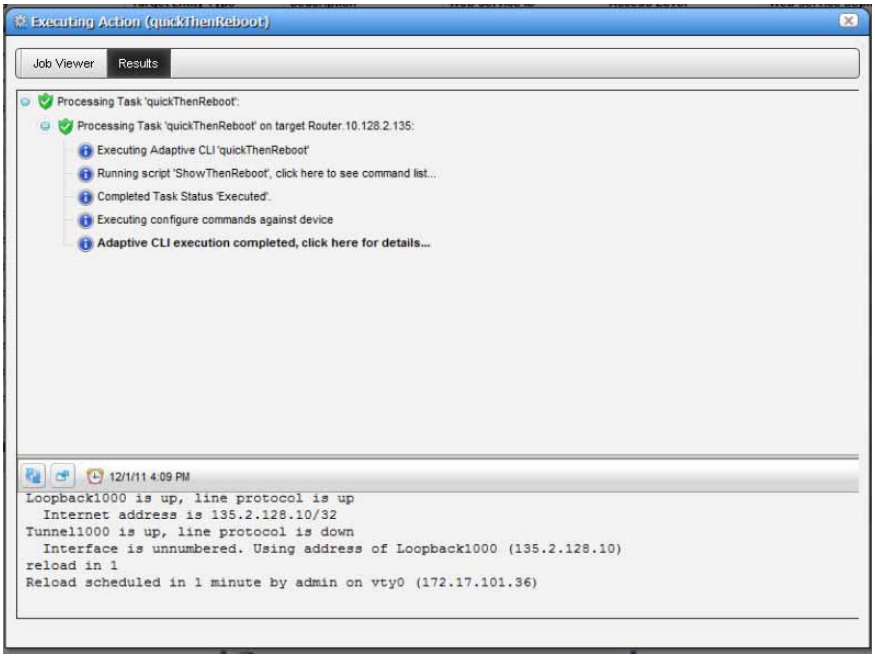
```
show run
reboot 1 minute
```

3 OpenManage Network Manager assumes commands are successful if a prompt appears without an error return. Default error tracking for most drivers provides all the error pattern matching you might need (testing the Adaptive CLI lets you know whether the device is addressed by a driver in “most”).

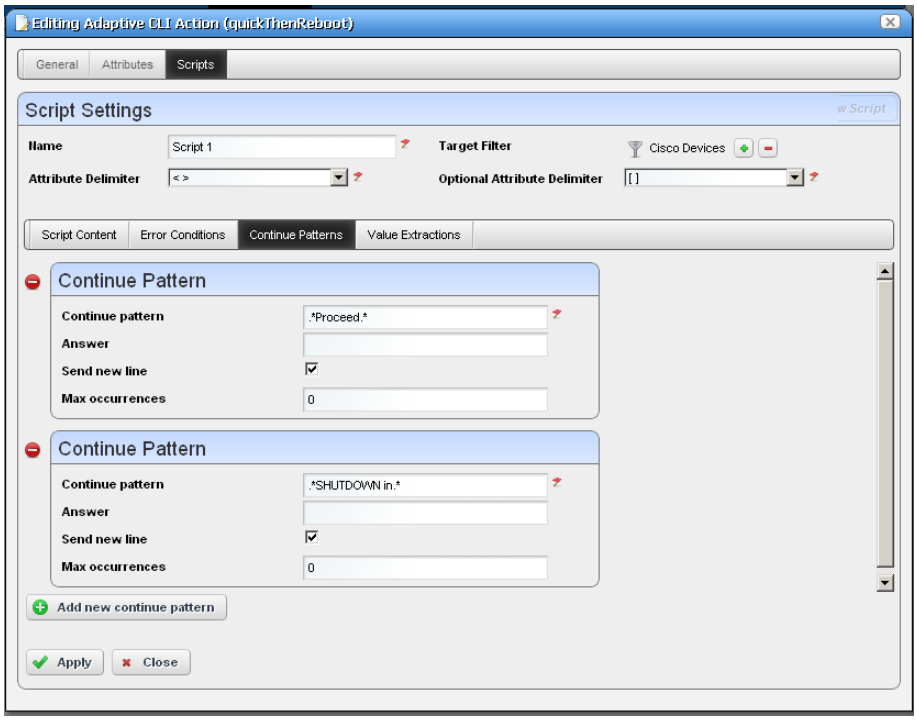
Use specific error pattern matching for cases where the driver does not detect the typical errors by default. As described in the Cisco Adaptive CLI Caveat on page 300, erroneous output appears if the error occurs on the reboot command.



4 When reboot is successful with a proper command sequence, the job screen displays the successful execution. See Cisco Adaptive CLI Caveat on page 300 for more about continuation prompts.



5 **Continue Patterns**—The following Continue Patterns section is an addition to the above example. It looks for the `Proceed` prompt so the Adaptive CLI can issue a new line to force the reboot. But the shutdown command follows the next prompt, so the shutdown command must be in another continue pattern to force the last line before a pause in output to be the router's prompt. The patterns are `.*Proceed.*` and `.*SHUTDOWN in.*` allowing any characters before and after the keywords to match.



Alternatively, this example could have a third command after `reboot` to force a new router prompt, but managing this problem with the continuation set seemed more straightforward.

Cisco Adaptive CLI Caveat

If you have not saved configuration changes for Cisco routers, then this Adaptive CLI fails. For sake of this example, such a failure is the correct response. However, if the Adaptive CLI needs multiple confirmations you can just add more with their responses as appears in the Continue Patterns described above.

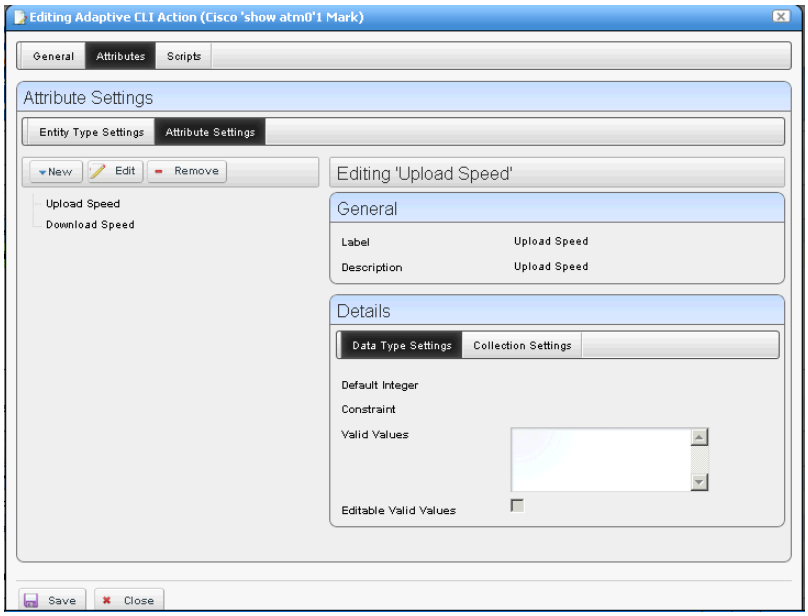
Example 4 - Adaptive CLI To Extract Upload / Download Speeds

The following describes an example Adaptive CLI configured to extract upload and download ADSL speeds from a Cisco Router. To create this example, follow these steps:

1 Right-click to create a new Adaptive CLI in the Actions portlet.

2 Name it and configure the Adaptive CLI in the General screen. Since these are generic settings described elsewhere, the details do not appear here.

3 Create attributes to extract. In this case, we configure Upload Speed, and Download Speed as integer attributes, with a name, description, and nothing else.



Notice, however, that you could configure validation for extracted attributes if you liked in this screen.

4 Create a new schema for these attributes. Schemas are helpful if you are creating several Adaptive CLIs (create, destroy, update, and so on) with the same set of attributes. With schemas, you are sure the attributes are configured exactly the same.

5 *Save* the configured attributes, click the *Script* panel

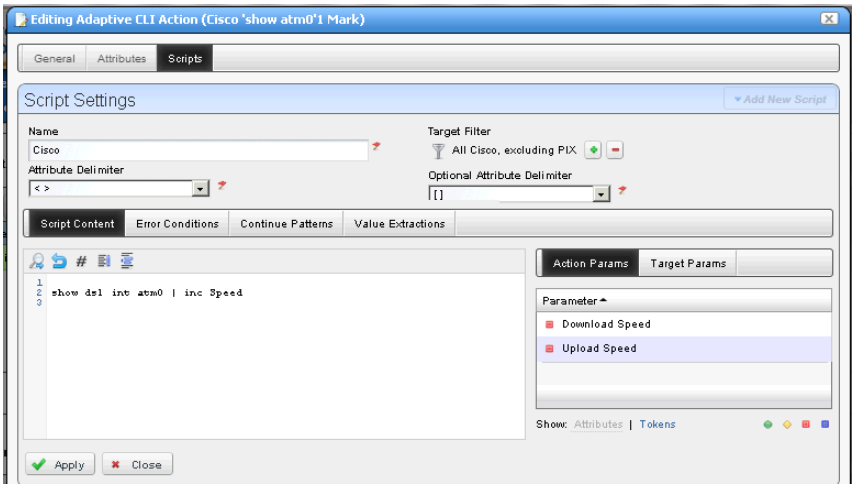
6 Enter the script. This extracts upload and download speeds from a Cisco device based on the output from this command (the script's contents):

```
show dsl int atm0 | inc Speed
```

This command shows dsl, grepping (`inc`) for the unique line beginning with `Speed`. The line for which this script searches looks like this:

```
Speed (kbps): 544 0 256 0
```

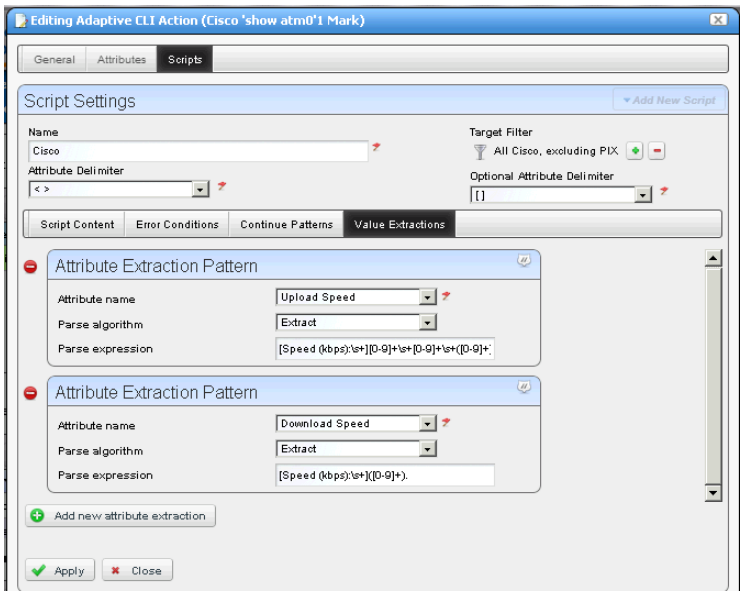
The attributes configured previously appear beside the script panel, but are not part of the script, even though that possibility might be useful for another Adaptive CLI. The current attributes are for extraction from the script results.



NOTICE

The filter at the top of this panel can limit the devices scanned by the Adaptive CLI to extract data. If you have a specific device or group of devices against which you plan to test this script, it would be a time saver to create the filter first.

7 Click the *Value Extractions* panel within the Scripts screen, and configure an extraction regular expression for each of the two values.



Click the green plus to add the second attribute.

With the pick lists, select an attribute, and that you want to extract (that is, within which you plan to store a value), then enter the regular expression to match its target value. Here are those attribute / regular expression pairs:

- Download Speed (the first integer in the output)

  `[Speed (kbps):\s+]([0-9]+).`
- Upload Speed (the third integer in the output)

  `[Speed (kbps):\s+][0-9]+\s+[0-9]+\s+([0-9]+).`

NOTICE

You can use free regular expression testers to debug these expressions. See Regular Expression Testing on page 306.

8 Apply the edits you have made to script and extractive regular expressions, then *Save* the Adaptive CLI.

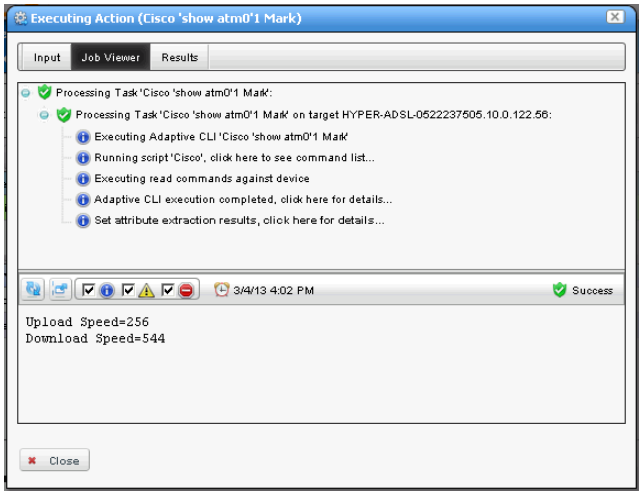
9 Right-click the Adaptive CLI and *Execute* it.

10 Select the target device(s).

11 Confirm the execution. The screen that appears before you click *Execute* again would have fields if you had a script with input parameters.

12 The *Results* panel appears to advise whether the script ran successfully, displaying its output.

13 Click *Job Viewer*, and arrange that panel so it displays informational messages by clicking the icon next to the date / time display. Check the checkbox next to the blue informational circle, and click the *Refresh* icon to the far left.



14 Click the last informational message (*Set attribute extraction results...*) and the extracted attribute values appear in the data panel at the bottom of the screen.

Example 5: Monitor Text Values

Create an Adaptive CLI with the following to monitor layer 1 and layer 2 status:

- integer attributes: layer1status, layer2status
- Script to produce the output: `show isdn status`

  Here is the output to match:

  ```
  Layer 1 Status:
  ACTIVE
  Layer 2 Status:
  TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
  ```
- Attribute Extraction Pattern:

```
layer1status / Match / (Layer 1 Status:\n\s+ACTIVE)
```

- For layer2status, the regular expression is like

```
(Layer 2 Status:\n\s+TEI = \d, Ces = \d, SAPI = \d, State =
   MULTIPLE_FRAME_ESTABLISHED)
```

Create a monitor to display the result of regularly running this Adaptive CLI on selected targets, and display its result in a dashboard.

NOTICE

Don't forget to enable the attributes in the monitor!

Monitoring Upload / Download Speeds

Once you have configured this Adaptive CLI, you can monitor its operation. Follow these steps to configure the monitor for the How to: Create a Monitor for the External Script Adaptive ACLI:

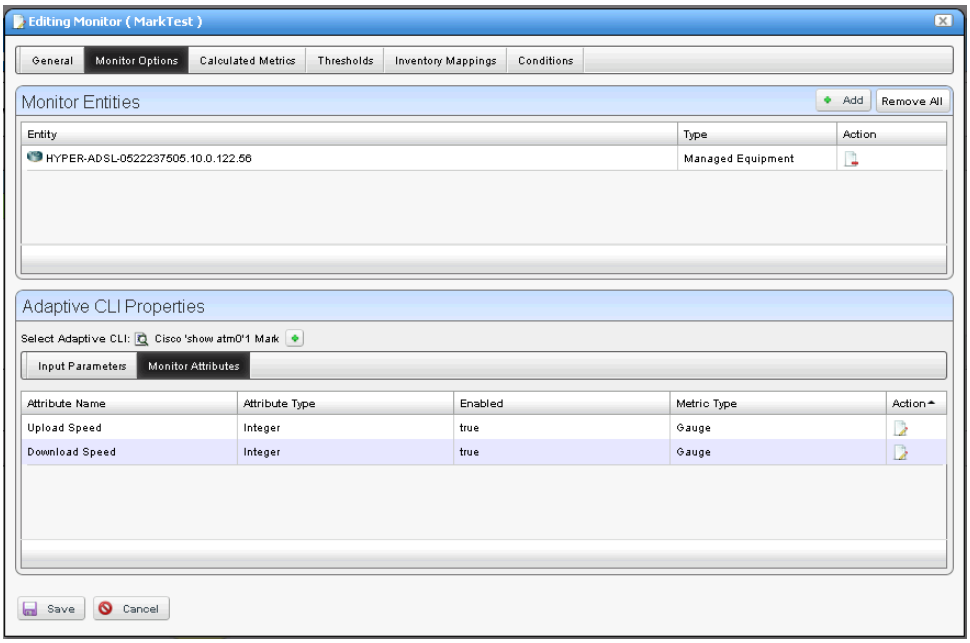
NOTICE

If you are testing, make the monitoring more frequent than you might in a production system so you can see if the data is available as expected. You can always change this after you have successfully tested the monitor.

1 Right-click in the Resource Monitors portlet to create a new monitor.

2 Enter the default name, and interval for the monitor in the *General* panel.

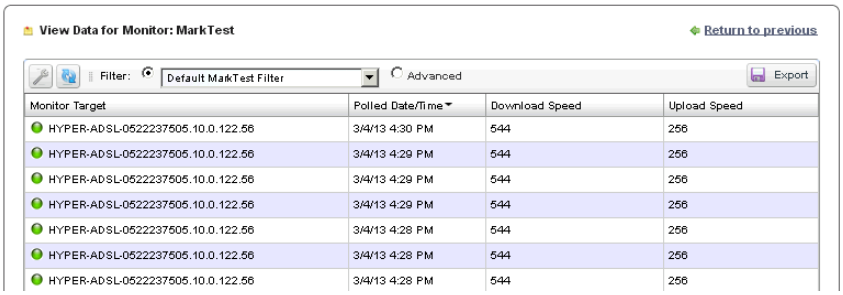
3 In *Monitor Options*, select the Monitor Entities (target devices) with the green plus, and subsequent screen.



4 In the same screen, elect to *Enable* the extracted Monitor Attributes with the editor icon to the right of the listed attribute. Notice you can also elect to report the attribute as a Gauge, Counter or Boolean. We selected Gauge.

5 Click *Save*.

6 Right-click the saved monitor to *View Monitor Data*.



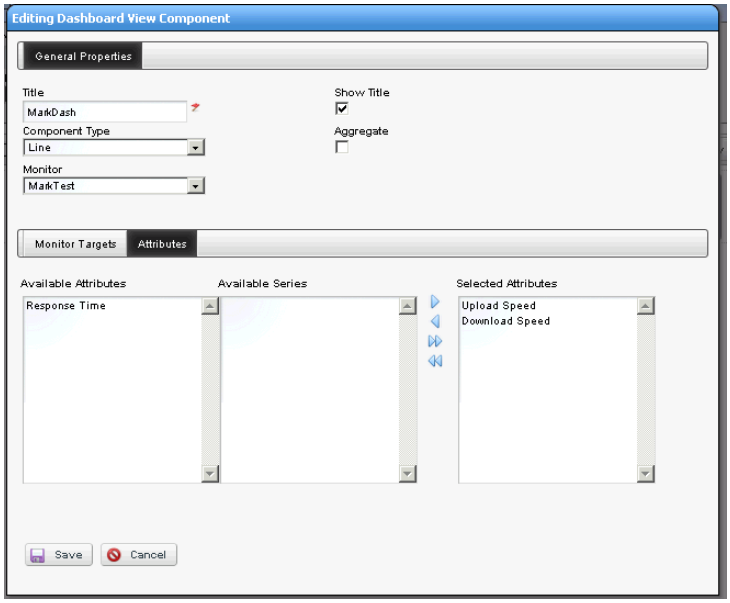
You may have to click the wrench icon to configure the columns that appear so this screen displays the extracted attribute information. You should see the extracted values displayed in a table.

Configure a Dashboard for Your Monitor

Finally, if you want to configure a dashboard to display your monitored data graphically, follow these steps:

1 Go to the Dashboard portlet, and right-click to create a Custom dashboard.

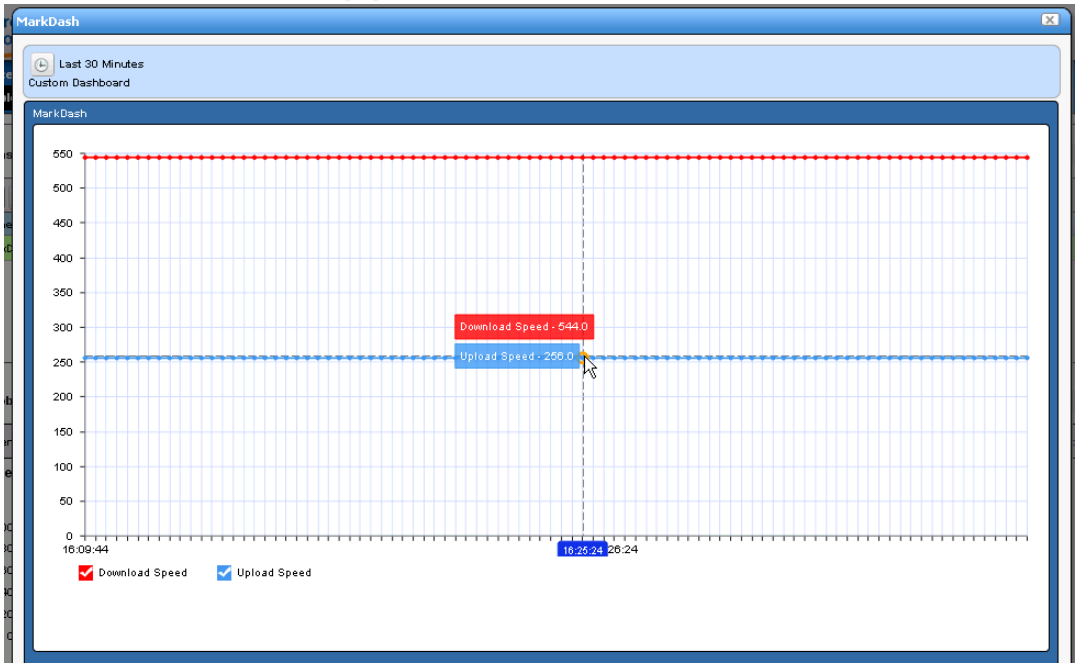
2 Enter the default data (name, retention policy, and so on) and configure the device and monitor selection by editing the panel(s) you want to display with its editor icon in the upper right corner.



Notice that you can select not only the monitor, but also the target(s) and attribute(s) to display. Here, we have selected the Upload / Download Speed attributes configured in the How to: Create a Monitor for the External Script Adaptive ACLI.

3 *Save* the configured dashboard.

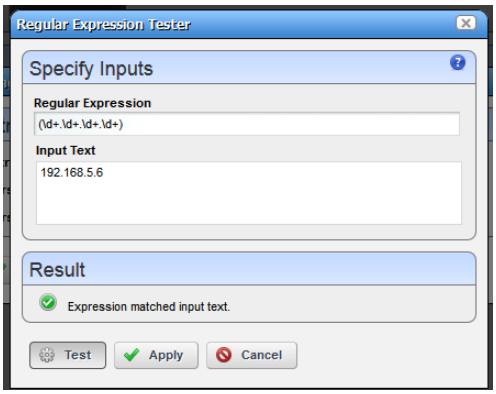
4 Right-click the dashboard in the Dashboard Views portlet and view it in one of the options available (Full Screen / Popup).



Notice that you can hover your cursor over a node in the graph and see all reported values for that node.

Regular Expression Testing

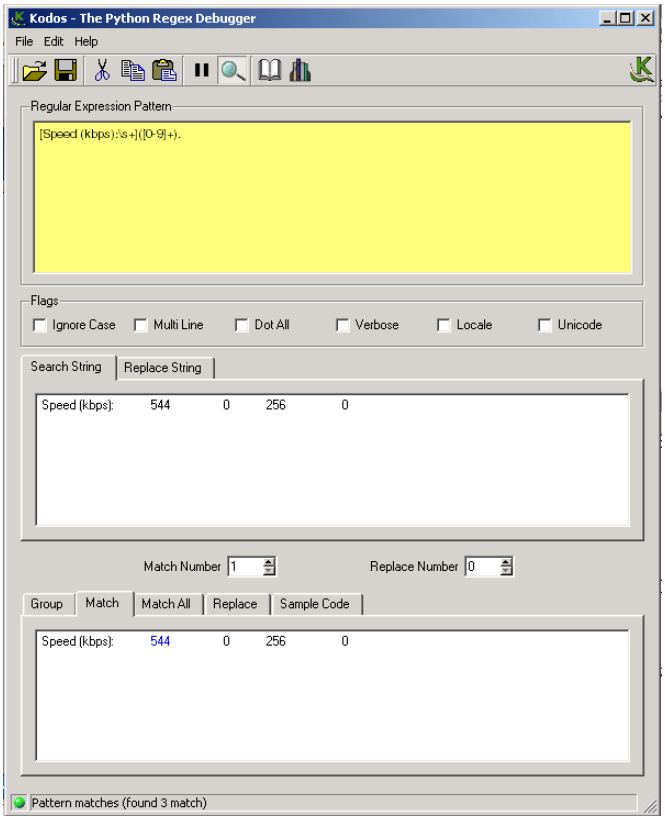
You can test regular expressions in OpenManage Network Manager by clicking the icon in the



upper right corner of screens like the one for Attribute Value Extractions in the Adaptive CLI editor.

After entering the *Regular Expression* and the *Input Text*, click the *Test* button to see whether the expression extracts the text you want. Revise it if it does not match, or click *Apply* to accept the expression and enter it in the editor.

Several applications, some free, are helpful to validate regular expressions too. These include websites (regexr.com, for one). These may also be helpful when trying to match a particular number and phrase in the Adaptive CLI and other output. In this example, we used Kodos to test various iterations of our regular expressions.



Enter the regular expression in the top panel (note the helpful hints from the online help), the output to scan in the middle panel, and the match appears in the bottom panel. Note: this application is not supported by OpenManage Network Manager developers.

Regular expressions include metacharacters to instruct the program how to treat characters it encounters. These include the following: ^, $, . , | , { , } , [,] , (,), *, +, ? , \. If you want to match one of these metacharacters, you must prepend a backslash (\). So to match a literal question mark, rather than instructing regular expression matching to match 0 or 1 of a previous expression, you must enter \?. To match a continue prompt that says `Proceed? (y/n)` you must escape three characters in regular match expression, like this `Proceed\? \(y/n\)`

Scheduling Actions

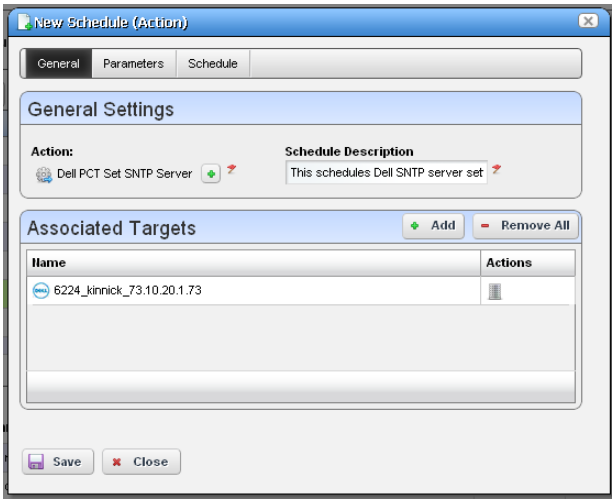
You can schedule actions with a right-click in the Actions portlet or the Schedules portlet. This opens an editor with the following screens:

- General
- Parameters
- Schedule

See Schedules Portlet on page 649 for more scheduling actions with that portlet. Schedules created in the Actions Portlet also appear in the Schedules portlet.

General

This screen lets you identify the scheduled item and its targets.



This has the following fields:

General Settings

Action—Identifies the action being scheduled.

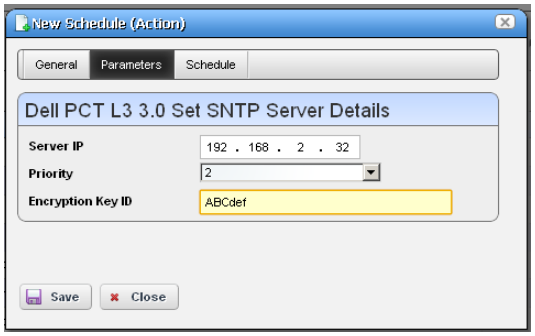
Schedule Description—Identifies the schedule.

Associated Targets

Click the *Add* button to select target equipment. You can remove listed equipment with the icon to the right of listed items or with the *Remove All* button.

Parameters

This screen's configuration depends on the selected action you are scheduling. Many actions have no parameters, so this tab is disabled. Enter the parameters for the action you are scheduling.



Hover the cursor over fields to make their description appear in a tooltip.

Schedule

This screen is a standard scheduler screen, as described in Schedules Portlet on page 649.

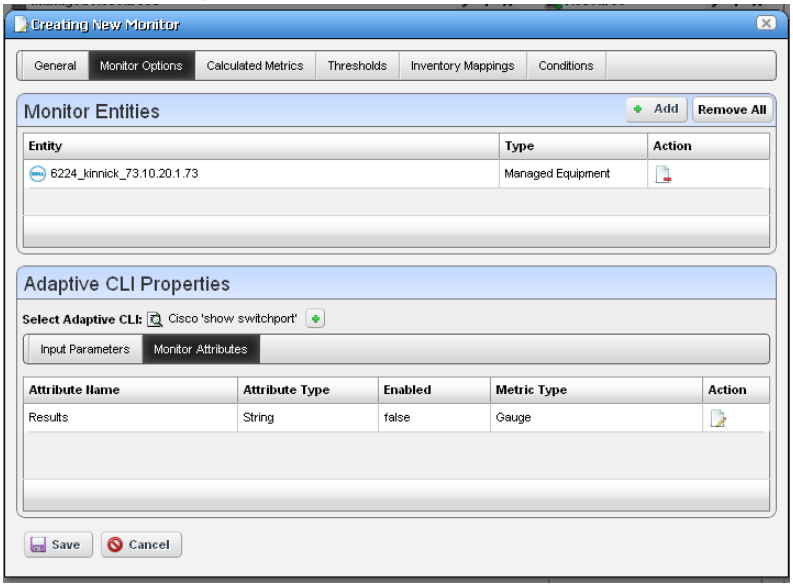
Comparison

Selecting (ctrl+clicking) two Adaptive CLI runs within the *Execution History* portlet lets you compare the two execution results. Right-click and select *Compare*.

Lines that differ between the two configurations appear highlighted green. Lines that are missing in one, but that appear in another appear highlighted red. Added lines appear highlighted in yellow. Use the right/left arrows at the bottom of this screen to page through the side-by-side comparison.

Active Performance Monitor Support

You can monitor Adaptive CLI execution results with Active Performance Monitor. To do this, you must select Adaptive CLI as the monitored type when creating a new performance monitor (see Resource Monitors on page 169), then select a target entities (with the *Add* button in the top panel) and a particular Adaptive CLI (with the green plus [+] in the Adaptive CLI Properties panel at the bottom of this screen. Click the *Edit* (page) icon to select the *Input Parameters* to monitor once you have selected an Adaptive CLI.

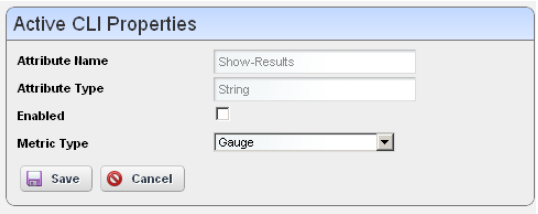


The user can choose an Adaptive CLI to monitor and may have to configure both its input values and metric type for each output attribute. The Input data depends on what the Adaptive CLI attributes have configured.

Input Parameters

In Active Monitoring, all attributes of the schema appear in the *Input Data* for user-entered values. You must enter the data necessary for all selected targets' scripts. To enter data, click *Edit* and then enter values. Clicking *Apply* switches the panel back to read-only mode. You must click Save to preserve input or output data configurations.

Monitor Attributes



Configure Adaptive CLI output attributes for monitoring in this tab in the lower panel of the Monitor Editor screen. You can monitor only exposed attributes of numeric or boolean types. To change metric type, select the row and click the *Edit* button to its right.

An Adaptive CLI Properties screen appears that reminds you of the *Attribute Name*, and *Attribute Type*, where you can *Enable* the attribute monitoring, and select *Gauge*, *Counter* or *Boolean* buttons to the right of this panel to configure the metric type of the selected output data.

These attributes default to the metric type *Gauge*. Adaptive CLI is where you define these attributes, but you must select their metric type settings on this screen if it is something other than the default.

Click *Save* to preserve your configuration, or *Cancel* to abandon it and close the editor screen.

How To:

Create a Monitor for an External Script

The following steps describe creating a monitor for an external command configured as an Adaptive CLI (ACLI). Several Perl scripts appear in this performance\scripts directory by default. You can try others in addition to the `http_test.pl` script in the example.

Create the Adaptive CLI

1. Right click in the Actions portlet, and create a new *External Command* ACLI
2. Make a new attribute schema with attribute: Status (integer)
3. In Scripts, enter the following as Script Content:

   ```
   perl "[installation path]\owareapps\performance\scripts\
       http_test.pl"[_EquipmentManager_IP_Address]
   ```

   The variable [_EquipmentManager_IP_Address] provides the target device's IP address, and comes from the *Target Params* tab, where you can find other such variables. If you want to test this script on an HTTP process on a device not under management, just to see the outcome, enter a known URL instead of that variable (like www.testsoftware.com), and run the script to see its output. (You will still have to select a target managed object to run the script, even though it is not part of the command line.)

   Since this is an example, use your [installation path] instead of those words.

4. In the Value Extraction panel enter the following:

   ```
   ^\{(\d+)\}.*
   ```

5. Click Apply
6. Click Save
7. Right click and *Execute* the ACLI to test it.

How To:

Create an Advanced Script Monitor Example

The following monitors an external Adaptive CLI example of setting up a simple process monitor using ACLI:

1. Make sure Perl is installed (and Windows has restarted after installing it), and check that the required libraries (`Info.pm` and `WMI.pm`) are in place. Your directory may vary; with 64-bit Strawberry Perl the locations are:

   For Info.pm:

   `C:\strawberry\perl\vendor\lib\Win32\Process`

   and for WMI.pm:

   `C:\strawberry\perl\vendor\lib\Win32\Process\Info`

   The process folder is attached to this document with proper structure. Put it in `C:\strawberry\perl\vendor\lib\Win32` and you are ready to go.

   NOTICE

   Here are the URLs where you can download these libraries:
   http://search.cpan.org/~wyant/Win32-Process-Info-1.018/lib/Win32/Process/Info.pm
   http://search.cpan.org/~wyant/Win32-Process-Info-1.019/lib/Win32/Process/Info/WMI.pm

2. Put `process_check.pl` in the proper directory. For Windows the default is `[installation root]\owareapps\performance\scripts`.
3. In your actions portlet, import TEST_ACTION.xml.
4. In your monitors portlet, import PROCESS_UPTIME_MONITOR.xml.
5. Even though the monitor and Adaptive CLI do not technically need one, select any target a dashboard can track. This permits execution of the Adaptive CLI.
6. In your dashboard views portlet, create a new custom Monitor Dashboard for whatever device(s) you decided to monitor, you will see Status as one of the tracked metrics (1 for up, 0 for down). You can use it as you would any other metric in OpenManage Network Manager to track, graph, and so on.

By default this script and monitor track whether `notepad.exe` is running, but you can have it track anything by editing the monitor. Go to Monitor Options > Adaptive CLI Properties, and you can edit the *Process Name* variable to be any other process.

Extra credit: Modify the script to track multiple applications.

process_check.pl

```
#!/usr/bin/env perl
use Win32::Process::Info;
$processname=$ARGV[0];
$found = 0;
$pi = Win32::Process::Info->new ();
@info = $pi->GetProcInfo ();   # Get the max
@info = grep {
 print $_->{Name};
 print "\n";
 if ($_->{Name})
 {
```

```
if ($_->{Name} eq $processname)
{
$found = 1;
}
 }
} $pi->GetProcInfo ();
if ($found == 1)
{
print "Process " . $processname . " is running! 1";
}
else
{
print "Process " . $processname . " is not running! 0";
}
```

TEST_ACTION

This action's name is *TestExternalScript*. It has two attributes, *Process Name*, a string, and *Status*, an integer. It stores the retrieved process' status in the *Status* integer, and takes *Process Name* as a required input. It refers to the process_check.pl script as an external command in its *Scripts* tab. Here is the syntax:

```
perl [installation root]\owareapps\performance\scripts\process_check.pl
   <Process_Name>
```

In addition to referring to the script, this Adaptive CLI extracts the status from the script's run. Essentially it looks for 0 (down) or 1 (up) with the following regular expression in the *Value Extractions* tab:

```
(\d)$
```

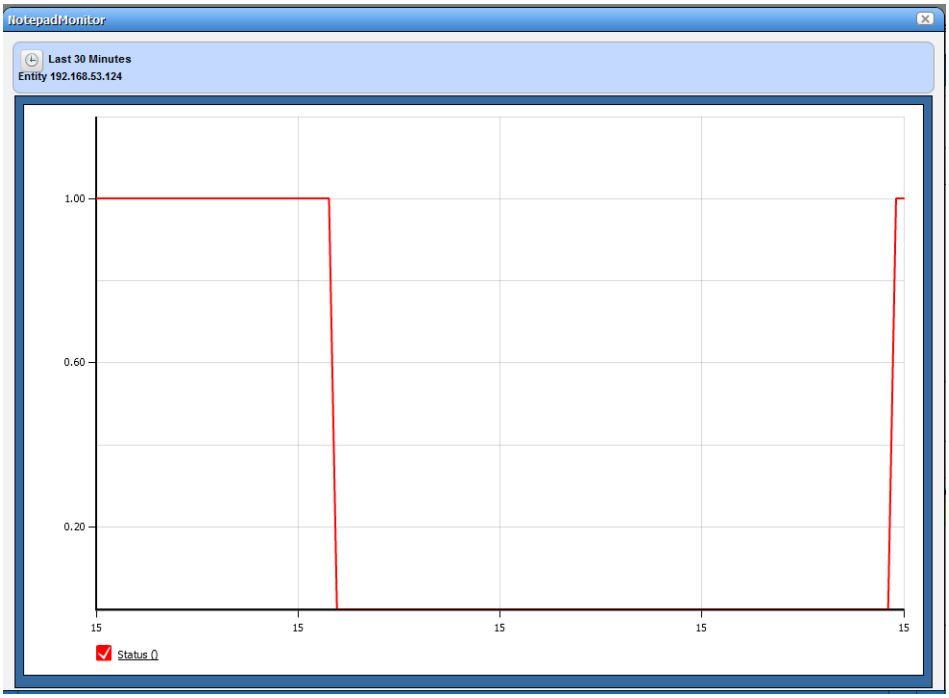
Note: `[installation root]` is an example only, not a legitimate part of the path.

PROCESS_UPTIME_MONITOR

This monitor's name is *ProcessUptimeMonitor*. It refers to the TestExternalScript (TEST_ACTION) Adaptive CLI. Notice that the *Process Name* attribute defaults to notepad.exe, and the Monitor Attributes tab contains the *Status* attribute.

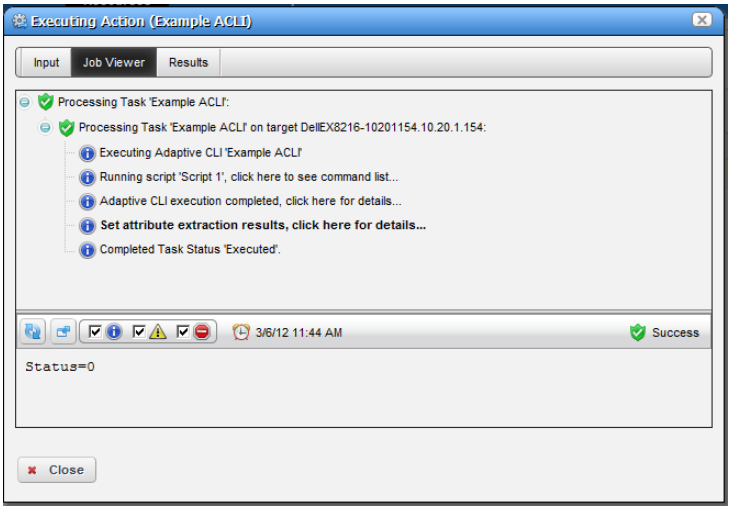
Monitor Dashboard

To see the result of your monitoring, create a custom monitor dashboard with the PROCESS_UPTIME_MONITOR as its target monitor, and the desired target device as its target device.



You can then see the process' activity over time when you launch the dashboard.

7 Look in Job Viewer for the results.

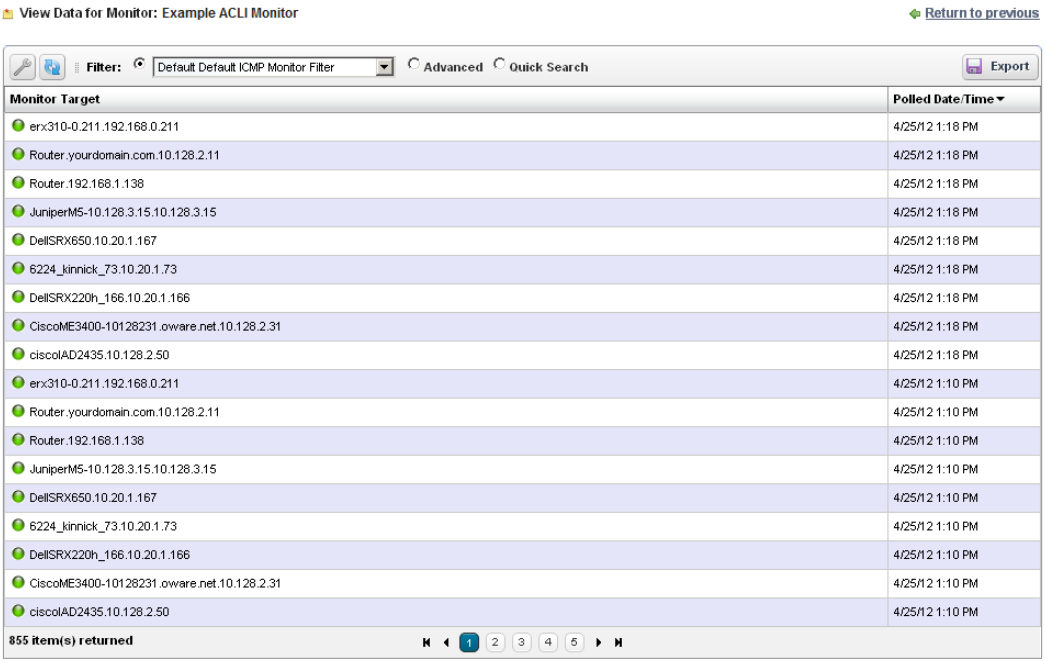


Click *Set attribute extraction results, click here* to see the results appear in the bottom panel. Notice also that you must check informational messages for all these to appear, and that several additional sets of messages besides the extraction results appear.

Create a Monitor for the External Script Adaptive ACLI

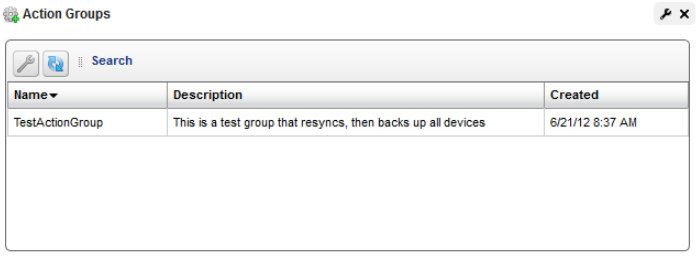
Now that you have verified the script is working, you can create a monitor to see how this attribute is doing.

1. In the Monitors portlet, create a new ACLI Monitor
2. Uncheck *Update Network Status* (recommended since the ICMP monitor is already doing this)
3. You may want to test your monitor, in which case, change the monitoring interval to 30 seconds. Re-edit it to configure it with the interval needed for your production system.
4. In *Monitor Options* select your example monitor configured previously.
5. Confirm that *Monitor Attributes* displays the Status attribute configured previously.
6. In the *Conditions* tab of the Monitor Editor, create "Status Up" condition, with the severity of *Informational*, and check *Alert*.
7. Create a criterion which is Status = 0.
8. Save this condition
9. Create a new Condition called "Status Down"
10. The criterion is Status = 1
11. Apply and Save
12. Save your monitor.
13. Right-click to select *View Monitor Data*, and you can see the results of your efforts.



Action Groups

The Action Groups Portlet lets you configure several actions with different targets, order their execution, and execute actions against these groups of targets all at once.

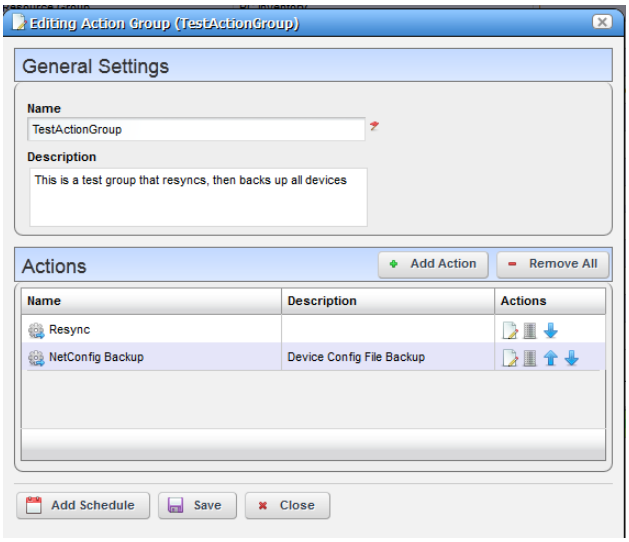


Right click within this portlet to create a New Action Group, Edit an existing, selected one, Execute the selected Action Group, view the Audit trails for the selected group, or Schedule the selected Action Group. You can also share action groups with others users on your system.

The Action Group Editor on page 315 configures new or existing actions. See also Configure an Action Group on page 316 below.

Action Group Editor

This editor lets you create or edit an Action Group.



It has the following fields and buttons:

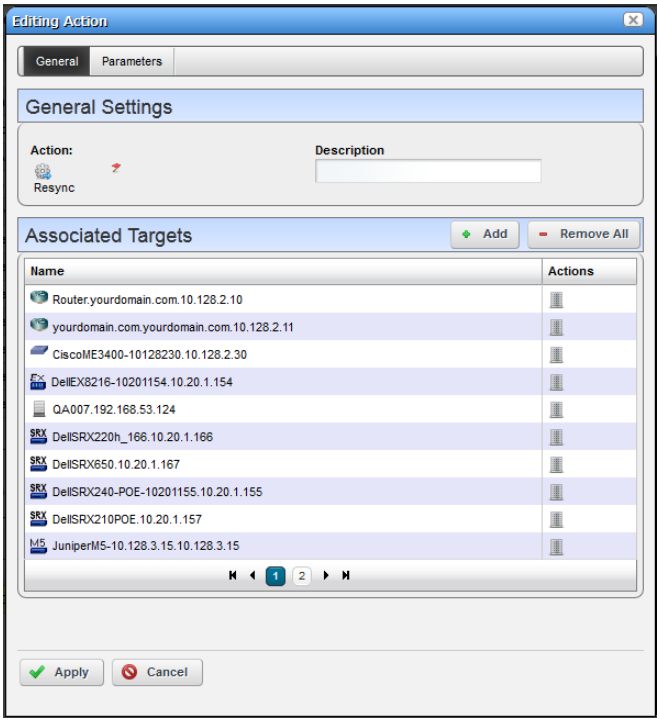
Name—A unique text identifier for the Action Group

Description—A text description for the Action Group

Actions

This portion of the screen lists all added actions. Use the *Edit this entry* icon (pencil and paper) to edit individual actions, or the *Delete this entry* icon to delete individual actions. The up/down arrows configure the order of execution (top first). Editing an entry opens the editor described in *Add Action* below.

Add Action—This opens an Action Editor where you can select the Action that is to be a member of the group, its Target devices and any Parameters associated with the Action.



Use the *Add* button to add Associated Targets, and the *Delete this entry* icon to delete any added by mistake. Click *Apply* to accept an added (or edited) Action. When you do this the list on the Actions panel of the Action Group Editor changes to reflect the changes you have made.

Remove All—Delete all Actions.

Click *Save* to create the Action Group. Once you have saved the group, you can right-click to *Execute* it manually. You can also click *Add Schedule* to schedule its execution. Clicking *Close* ends your editor session without saving any new Action Group, or changes you may have made to an existing one.

NOTICE

When you execute an Action Group, the Results view displays a list of targets on the left, and results for the selected target on the right. Click on a different target to see the target's results.

How To:

Configure an Action Group

Follow these steps to configure an Action Group

1. Right-click in the Action Groups portlet, and select *New*.
2. Name the Action Group, and optionally type a Description.
3. Click *Add Action*.

4 Select an action (with the green plus at the top of the screen), and optionally add a Description in the field to the right of the selection.

5 To associate devices with this action, click the *Add* button in the Associated Targets panel, and select the device(s).

6 Click *Done*.

7 Review the selected devices, and click *Apply* once that list is correct.

8 Review the added Actions, and insure they are in the correct order. Re-order them, if necessary.

9 Click *Save* to preserve your new Action Group.

10 Right-click and select *Execute* to test the Action Group.

11 If appropriate, and execution is correct, right-click to *Schedule* for this Action Group. Configure its occurrence in the Schedule panel of the screen that appears next, and *Save* that schedule.

Troubleshooting Adaptive CLI

The following issues can prevent the correct completion of Adaptive CLI execution.

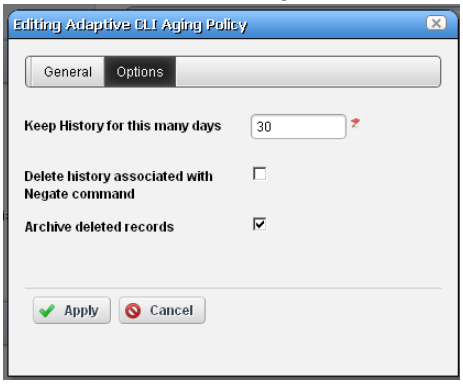
Connectivity—The device can be offline. To detect whether this is true, right-click the device in the Managed Resources portlet and *Direct Access* > *Ping* it.

Incomplete Discovery—If the device is online and still does not respond to Adaptive CLI, you may have only partially discovered it. Right-click the device in the Managed Resources portlet and select *Direct Access* > *Terminal*. If that menu option does not exist, it is only partially discovered. Right-click to edit the device, and add a Telnet Management Interface and Authentication in those two tabs of the editor.

Timeouts—Adaptive CLI timeouts may occur because of an unresolved *Continue* prompt. See *Continue Pattern* on page 281 for instructions about how to resolve such things. Depending on the device, you may also configure the device itself not to emit patterns that need a response.

Adaptive CLI Records Aging Policy

You can use OpenManage Network Manager's aging feature to preserve Adaptive CLI information. Click the Redcell > Database Aging Policy (DAP) node of the Control panel, and click the default *Adaptive CLI DAP* and click the edit button on its right.I



After filling in the *General Info* tab, the *Parameters* screen lets you configure the following:

Keep History—Enter the number of days to retain the history in the database.

Delete history associated with Negate command—Check to remove archived records associated with *Negate* (described under General on page 270).

Archive Deleted Records—Check to have deleted archived records saved as a file (configured in the *General Info* parameters too).

Web Service Deployment Features

Right-clicking in Actions Portlet supports deploying actions as web services, as described in the following section. Web services are typically the concern of administrators, not operators. Administrators using these features are expected to be familiar with the web service technology they configure. Refer to the *Web Services Guide* for more about WSDL.

Deploy Web Service—You can select one or more Actions to deploy as a web service. You must assign each selected activity a unique Web Service ID, that can ultimately appear in a column in the Activities Manager screen. The screen that appears after you select this item lets you assign this ID for each activity connected to the web service. This screen's appearance depends on the web service you select.

The Web Service ID can contain only alphanumeric characters and underscores (_) and must start with either a letter or underscore. This ID represents the input data class (or type) of the activity. It defaults to a valid name reflecting the activity name. You can change the default. Upon successful deployment, the Web Service IDs of the deployed activities appear in the manager. You can then export the WSDL file for code generation and web service invocation.

NOTICE

You can see deployed Axis2 web services listed in the screen at http://[application server IP address]:8089/axis2/services/listServices. These may take a little time to appear, so be patient. If you have been patient, and they still do not appear listed, you may have to clear your browser's cache. Clicking the *Activity* link once they appear displays the WSDL.

Undeploy Web Service—Select one or more activities to undeploy from web service. When successful, the Web Service IDs of the undeployed activities are cleared from the manager. Undeployed activities are also no longer accessible for web service requests.

Export WSDL—After deploying and undeploying activities, you may want to export the WSDL file for client code generation. The WSDL file contains all the data class types for web service execution.

All activity web service client code shares a common web service method: `TaskSvcExecute`, which takes in `TaskSvcExecuteInParams` as input data and returns `TaskSvcExecuteOutParams` as output data. The following describes the input and output data:

Input Data:

Async—A Boolean type. If true, indicates an asynchronous (not synchronous) request. Asynchronous requests return immediately with a job ID, while synchronous requests await completion of the web service execution before returning job IDs. Either way, you must then use the Job web service to examine the results.

TargetOID—A string representing the ID of the Target Entity Type.

TaskData—This is the base parameters class to be replaced by the activity-specific extended data class (namely the Web Service ID) associated with the activity execution.

Output Data:

JobID—This is a unique ID string used for querying the results of an execution. The job web service is defined in `$OWARE_DEV_CACHE_CLS/ws.war/wsdl/Job.wsdl`. For results, the ParentJobID Status is one of the following values:

0 - Execution in progress (if async request)

1 - Execution succeed

2 - Execution failure

Status is an integer representing one of these values:

0 - Execution succeed

1 - Invalid input data

2 - Execution pending (for async request)

6 - Execution failure

8 - Invalid input target OID

NOTE:

The Status of the TaskSvcExecuteOutParams is different than the status of the job service.

TaskData—The base data class (same as input) returned as output data. Certain activities may produce output data.

11

Change Management / ProScan

OpenManage Network Manager's change management utility is ProScan. The ProScan utility which lets you scan stored configurations or Adaptive CLI show command output to verify that managed devices complyiance with company, department, or industry standards. The ProScan utilityThis application also automatically tracks all changes occurring to managed devices. You can report on user-specified values found in persisted backup configuration files for a group of devices. This lets network managers, security officers, and external auditors generate detailed audit trail documents to validate compliance with both internal standards (ISO 17799, NSA Guidelines) and industry regulations (Sarbanes-Oxley, GLBA, HIPAA).

Compliance reporting lets you specify a text string, regular expression, or optionally the generated configlet from File Management (NetConfig) for matching. Group results must be separated by device like Adaptive CLI Manager. When ProScan policies run, the application emits notifications whose contents depend on whether compliance was or was not maintained.

NOTICE

Your system may have several ProScan examples. You can use these as provided, or copy and alter them to suit your network.

How To:

Use ProScan / Change Management

The following outlines common use cases for this software, and the steps to achieve the goals of each case:

Goal: Regularly verify configurations are compliant

1. Create ProScan policy(ies) based on what indicates compliance. Right-click *New* > *Policy* in the ProScan portlet.
2. Specify the Name and Input source (based on Device Backup, Current Config, Configuration Label, By Date and Adaptive CLI Results)

3 Add Targets > Filter Option available for selecting Equipment/Group

NOTICE

The advantage of selecting dynamic device groups is that newly discovered devices of the selected type automatically become members of the group, so they are scanned too. A benign warning ("No proscan policies have target group(s)") lets you know you have not selected groups when you execute a ProScan policy without them.

4 Specify Proscan Compliance Criteria. Add Criteria. For example, that devices' SNMP communities *Do not contain* the following:

```
snmp {
community public {
```

5 Save.

6 Execute or schedule your created ProScan policies.

7 Any out-of-compliance devices throw an alarm, which you can email, or configure to trigger other actions (see the next use case).

Goal: If devices are not compliant restore compliant configuration

In addition to the steps in the previous section:

8 Create an event automation rule that responds to the redcellProScanFailureNotification event by executing the Netconfig Restore action. Typically you would select to restore the *Compliant* label. (28493)

If you have multiple device types you do not need to assign actions for each device, or even each device type. OpenManage Network Manager supports the assigned policies, so it knows which actions to do to that device based on which device sent the trap.

Avoiding Restoring Files for Trivial Differences

Because automated network updates, for example from NTP servers, can change configurations, you may want to tune this to avoid restoring files that differ only insignificantly. Do this by editing, or better overriding, the property file: ...`owareapps/netrestore/lib/nr.properties`. Alter the following property:

```
append.com.dorado.redcell.netrestore.backup.change.omit=
```

For example:

```
append.com.dorado.redcell.netrestore.backup.change.omit=,ntp clock-period
```

How To:

Configure ProScan Groups

If you have different ProScans for different device type, then you can run a ProScan Group and automatically scan even different types of devices. For more about this, see Creating or Modifying ProScan Policy Groups on page 339.

1 Right-click and select *New* > *Group*.

2 Specify the Proscan Policy Group Parameters.

3 Add ProScan Policies. These policies can be in multiple groups.

4 Add Targets. Notice that group targets appear in the "child" policies, grayed out. Child policies can add more targets.

5 Save.

6 Execute or schedule the group policies to run against the selected targets.



How To:

Do Change Management (Example)

The following describes an example use of Change Manager. This backs up a configuration file, modifies it, then scans the file for the modified text, and acts according to the result. The following steps describe how to do this:

1 Back up a device configuration. Select a device and click the *File Management* > *Backup* right-click menu in Managed Resources portlet.

2 Right click, and Export this backup to a file in the Configuration Files portlet.

3 Edit this config file, adding the word "MyTestContact" somewhere in its text that has no impact. For example, the snmp-server contact, or in comments. Some devices let you create descriptions within their configurations so you can enter a word without impact there.

4 Now import this edited file from the Managed Resources portlet after you have right-clicked on the same device from which you exported it. Renaming it something distinctive is helpful.

5 Right-click this file and *Restore* to the device. Since the name is a comment or description, it should not interfere with the device's operations.

6 Right-click the device and select *File Management* > *Backup*. This makes the MyTestContact file label Current.

To confirm MyTestContact is labeled Current, you can use an Advanced filter in the expanded Configuration Files portlet to view only Current labels.

7 Now, create a ProScan policy by right-clicking in the ProScan portlet, selecting *New* > *Policy*.

8 In the General tab, name this policy MyTestContactScan, and as an input, select the *Configuration Label* > *Current* label as the Input Source.

9 In the Targets tab, select the equipment from which you exported the config file.

10 In the Criteria tab, click *Add Criteria* enter *contains* MyTestContact as the *Match All of the following criteria*.

11 Click *Save*.

12 Right-click the new policy and select *Execute Compliance*.

13 The audit screen that appears should indicate *Success*.

14 Right-click and *Open* the MyTestContactScan policy, and change the Criteria to "does not contain" MyTestContact.

15 *Save*

16 Re-execute the policy.

17 The audit screen that appears should indicate *Failure*.

Alarms / Events

Once you have a ProScan policy that has failed, the redcellProScanFailureNotification alarm appears in the Alarms portlet. Success produces an event, not an alarm (visible in the Event History portlet) called redcellProScanClearNotification.

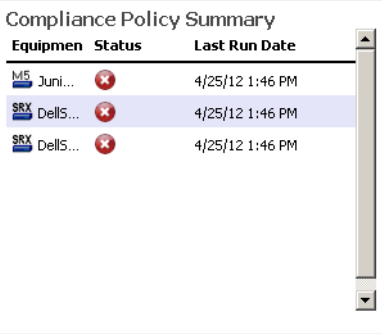
To create a response, create processing rules for the event/alarm (see Creating Event Processing Rules on page 95). For example, you could restore the Compliant-labeled configuration file if redcellProScanFailureNotification occurs, or send an e-mail to a technician, among many other responses.

Some Limitations in this Example

Note that this example does not change authentication, either for telnet or SNMP. If it did alter the SNMP authentication, you would have to create an SNMP authentication alternative before scanning could occur.

Compliance Policy Summary

This snap panel appears at the bottom of the expanded portlet described in Compliance Policy Summary on page 324. It catalogs the compliance policy's history and lists the *Equipment* scanned, a status icon indicating whether the run discovered equipment *in* (green) or *out* (red) of compliance. If you added equipment to a policy before it has run, you may also see a *Not Executed* (blue) status. Each run date for the policy and equipment combination selected in the list at the top of the detail panel screen appears as a row in this panel. You can also see compliance failure messages in OpenManage Network Manager's audit trails.



Compliance scans do not stop the first time they fail. They continue so all failures of compliance in the entire device configuration appear cataloged in the result.

Each time OpenManage Network Manager executes a compliance policy it stores a history record in the database. Similarly, edits to these policies update history records. When you edit a compliance policy to add/remove equipment, OpenManage Network Manager creates or deletes the corresponding history record. Every time OpenManage Network Manager executes the compliance policy, it updates the Last Run Date, Status and Details on the history record.

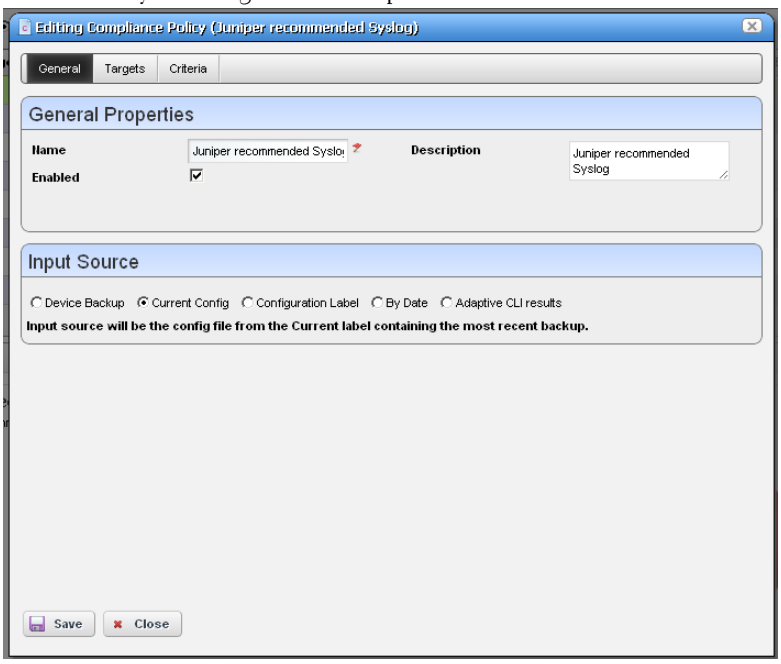
Groups

When you run a ProScan group policy, the history for the group appears in this detail panel just as it would for a single policy. History concatenates the results of the component policies, as does reporting. See Compliance and Change Reporting on page 349.

To see the Compliance Policy History, print a *Compliance Policy Violation* report from Report Manager.

Creating or Modifying a ProScan Policy

This series of screens lets you configure ProScan policies.



This screen has the following tabs:

- General
- Targets
- Criteria

The Compliance Policy Job Status screen displays progress of a ProScan policy as it executes.

CAUTION:
ProScan works only with text files; it does not work with binary configuration files.

If you have more than one type of device, you must typically have more than one ProScan policy to address each device type. To run more than one ProScan, so you can address multiple types of devices, create a ProScan group. See Creating or Modifying ProScan Policy Groups on page 339.

General

This tab has the following fields:

General Properties

Name—An identifier for the policy (editable only when you click *New*, not on existing policies).

Enabled—Check to enable this policy.

Description—A text description of the policy. This also appears when the policy is listed in the manager.

Input Source

Use the radio buttons to select a source. Select from among the following options:

Device Backup—Retrieve the configuration from the device and scan it for compliance.

Current Config—The scan the current configuration backed up from the device.

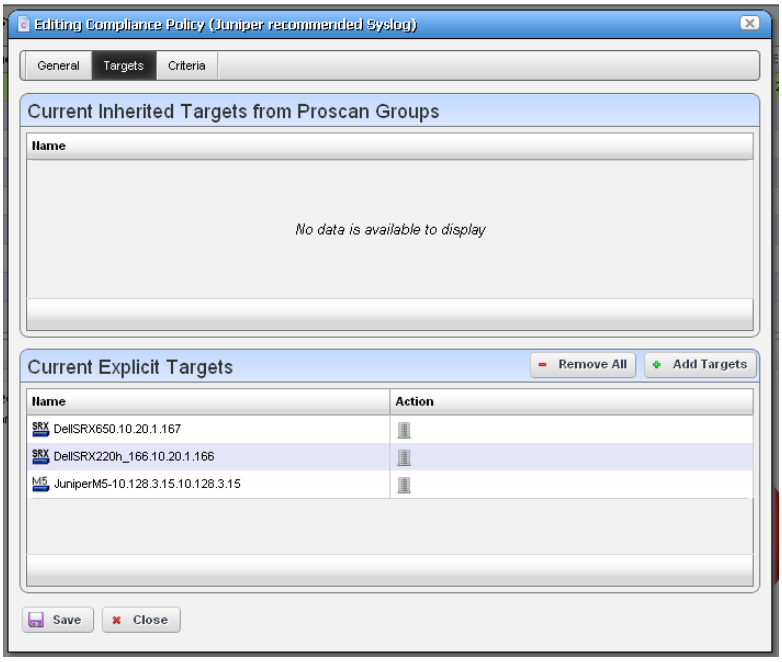
Configuration Label—Select the configuration to run against based on a label. This software automatically updates the *Current* label so it points to the most recently backed up configuration files.

By date—When you click this radio button, you can then select a configuration file backed up that precedes a specified date most closely in a selector that appears below the radio button. You can scan even historic configurations for compliance, with the *Based on Date* field. No validation ensures this date is the current one.

Adaptive CLI—Select a desired *Show* Adaptive CLI to scan the target device below the radio button. The policy configured scans the show results, and that show appears in the Audit screen.

Targets

The top of this screen (*Current Inherited Targets*) displays any targets inherited from already-configured ProScan Groups. Click *Add Targets* in the *Current Explicit Targets* panel at the bottom to select equipment that are targets to scan with this policy. You can also select listed equipment click the *Remove* icon to delete it from the list.



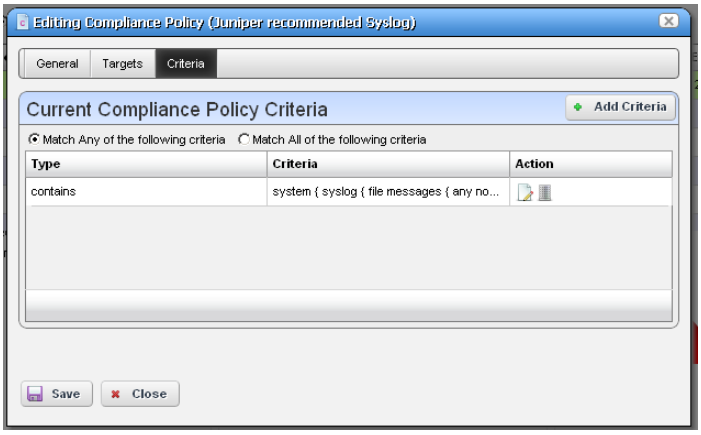
NOTE:

Use filtering in the subsequent selector screen to make individual selection easier, but do not forget this is *not* dynamic selection. You must assign policies whenever your managed environment adds new equipment.

To provide information for individual policies that are part of groups, this screen displays inherited group targets grayed out. See Creating or Modifying ProScan Policy Groups on page 339 for more about groups.

Criteria

This screen lets you filter configuration files based on text, or Regular Expressions. Click *Add* to open an editor line.



This screen ultimately determines whether the configuration file(s) for the selected equipment complies with the applicable policy. To create a policy, first select whether you want to *Match Any* (logical OR), or *All* (logical AND) of the criteria you configure with the radio buttons at the top of this screen.

See these sections for more about criteria:

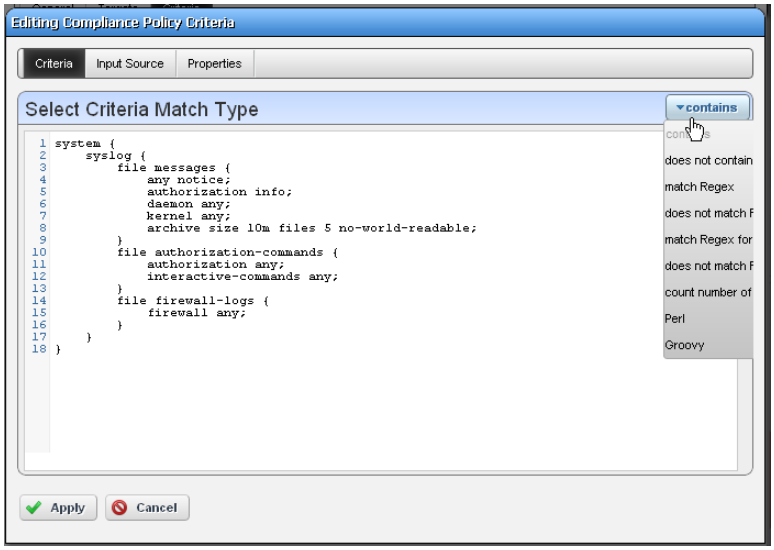
- Editing Compliance Policy Criteria
- Match Regex for each line
- Count number of occurrences
- Input Source Grouping
- Properties

For additional criteria information consult these sections:

- Create Source Group Criteria
- Regular Expressions
- Perl / Java (Groovy) Language Policies

Editing Compliance Policy Criteria

After clicking *Add Criteria*, use the pick list on the upper right to select an operation to select a criteria match type (*Contains*, *Doesn't contain*, *[does not] match Regex* (see *Regular Expressions* on page 333), *[does not]* Match Regex for each line, Count number of occurrences, Perl or Java (Groovy)). Specify the match string or regular expression (Regex) in the text editor below the pick list.



With the *Add Criteria* button, you can configure multi-criteria policies with several lines. For example, configure one saying a maximum of four lines containing `name-server` can appear (<5), in any order (Match Regex for each line), and another that says the configuration must contain `no ip domain lookup [domain]`.

Notice the radio buttons *Match Any of the following* and *Match all of the following*. Selecting *Any* means that if either of the lines matched the policy would succeed. Selecting *All* says that both lines must pass before the policy is successful.

For more complex scans, you can also enter Perl or Java (Groovy) language policies. See Perl / Java (Groovy) Language Policies on page 335 for details about these. The does not operators are just the negative of the match without does not.

Click the *Apply* green check button to accept your term, or the *Cancel* button to abandon your edits.

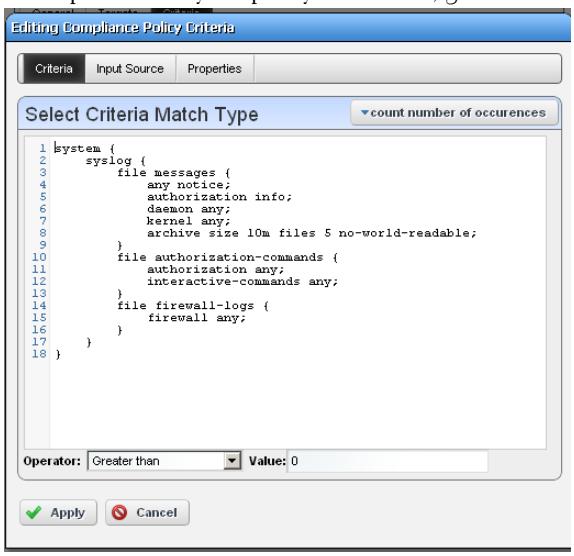
You can edit already listed compliance tests by clicking the *Edit* button (pencil and paper) in the list row. You can delete them by clicking the *Delete* button next to the criterion.

Match Regex for each line

In using this type of term, OpenManage Network Manager processes each line separately, comparing the input source to the match criteria. This returns a true value only if the criteria find a match in the source. The order of matching is not important since OpenManage Network Manager processes each line separately.

Count number of occurrences

This operator lets you specify a less than, greater than, or equal mathematical operator (<, >, =)



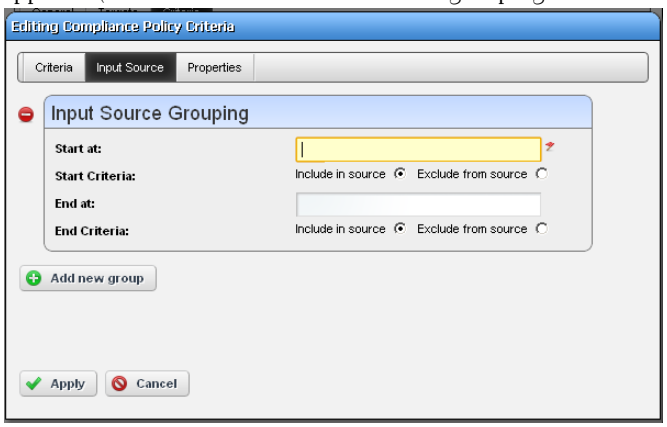
and a number of lines after you provide regex or string criteria with the operator and count value.

This returns true if the criteria (as a whole) match the input source count and operator combination. On the other hand, for example, if you choose a match criterion that includes =9 lines as the operator, and the scanned configuration has ten lines that match, the scan returns *false*.

Input Source Grouping

Adaptive CLI show commands and configuration files often have repeating sections or groups of parameters. OpenManage Network Manager scan configurations by section using *Start Criteria* and *End Criteria* Regex group criteria patterns. A configuration can contain multiple start and stops. This is especially useful when the criteria provided might occur multiple times in the input source but you want to find only the instances which are preceded by a particular line in the source.

Click *Add new group* in the *Input Source* panel in the Criteria editor, and the grouping editor appears. (Click the red icon to the source grouping's left to delete it.)



Enter the starting and ending regular expressions (*Start at* / *End at*), and elect whether the beginning or end of the source group includes or excludes what that expression matches. Click *Apply* to accept your edits, or *Cancel* to abandon them. You can create multiple group criteria. OpenManage Network Manager applies the group criteria in order, from top to bottom.

When you have defined a *Start* and *Stop*, OpenManage Network Manager finds the information between these. OpenManage Network Manager logically extracts the data from the main config (essentially creating sections) and then does the audit.

For example, if your configuration has one section of *router bgp* and multiple sections for each bgp neighbor, you can specify matches within each neighbor. Your policy can audit each router bgp section and each neighbor within each router bgp.

See Create Source Group Criteria below for an example of how to use these capabilities. Also, see Regular Expressions below for more about what match criteria are supported.

Properties

Checkboxes on this page configure whether the proscan match is *Case Sensitive*, or has *Multi-Line Support*. By default they are disabled. Check to enable them. If (upper / lower) case matters in what you are scanning for, check *Case Sensitive*. If you want to scan for a regular expression that spans more than one line, check *Multi-Line Support*. Lines do not have to be consecutive. For example, you could scan for hostname [line(s) intervene]ipv6.



How To:

Create Source Group Criteria

Here is an example of how you can use source group criteria. Suppose you want to scan for the following text:

```
neighbor 2.3.4.5 activate
neighbor 2.3.4.5 route-map allanRM01
```

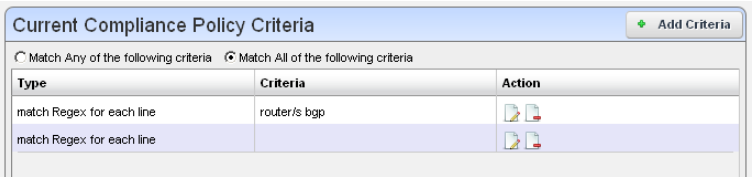
This is within the following configuration:

```
router ospf 888
 log-adjacency-changes
 redistribute bgp 88 metric 10010 metric-type 1 subnets tag 334 route-map
    allanRM02
 network 2.3.4.0 0.0.0.255 area 123
 network 2.3.5.0 0.0.0.255 area 124
 network 2.3.6.0 0.0.0.255 area 125
!
router isis
!
router rip
 version 2
 network 175.92.0.0
 no auto-summary
!
address-family ipv4 vrf VPN_PE_A
no auto-summary
 no synchronization
 exit-address-family
!
router bgp 88
```

```
 bgp log-neighbor-changes
 neighbor 2.3.4.5 remote-as 22
 neighbor description "This is Test"
 neighbor test-parameter xxx
 neighbor 4.5.6.7 remote-as 66
 neighbor description "This is Test"
neighbor test-parameter xxx
 !
 address-family ipv4
 redistribute connected route-map map-12
 redistribute static route-map hjlhjhjhjk
 redistribute ospf 888 metric 500 match internal external 2 nssa-external
    1 nssa-external 2 route-map allanRM03
 neighbor 2.3.4.5 activate
 neighbor 2.3.4.5 route-map allanRM01 in
 neighbor 4.5.6.7 activate
 neighbor 4.5.6.7 route-map allanRM02 in
 default-information originate
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf VPN_PE_A
 redistribute ospf 10 vrf VPN_PE_A match internal external 1 external 2
 no auto-summary
 no synchronization
 exit-address-family
!
```

In addition, within this configuration, you want to check if the target lines are present under each address-family in the *router bgp* section. To scan for this, follow these steps:

1. Select the *Match All of the following* radio button and enter both of the above lines as match criteria. Select the *Config Term* as *match Regex for each line*, so the order in which these lines appears does not matter.
2. *Add* a source group criterion to search for a section that begins with "routers bgp"—in regex: `routers\sbgp`. No end match criterion is needed. Click *Apply*.
3. Click *Add* to make another criterion. This time, the start is `address-family\s`, and the end is `exit-address-family`. Click *Apply*.
4. You should see both criteria listed in the editor



5. Applying the first group criterion finds the match (underlined) in the following:

```
router bgp 88
 bgp log-neighbor-changes
 neighbor 2.3.4.5 remote-as 22
 neighbor description "This is Test"
```

```
 neighbor test-parameter xxx
 neighbor 4.5.6.7 remote-as 66
 neighbor description "This is Test"
neighbor test-parameter xxx
 !
 address-family ipv4
 redistribute connected route-map map-12
 redistribute static route-map hjlhjhjhjk
 redistribute ospf 888 metric 500 match internal external 2 nssa-external
    1 nssa-external 2 route-map allanRM03
neighbor 2.3.4.5 activate
neighbor 2.3.4.5 route-map allanRM01 in
 neighbor 4.5.6.7 activate
 neighbor 4.5.6.7 route-map allanRM02 in
 default-information originate
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf VPN_PE_A
 redistribute ospf 10 vrf VPN_PE_A match internal external 1 external 2
 no auto-summary
 no synchronization
 exit-address-family
!
```

6 Applying the second group criterion on the above result divides the source:

Source 1:

```
address-family ipv4
 redistribute connected route-map map-12
 redistribute static route-map hjlhjhjhjk
 redistribute ospf 888 metric 500 match internal external 2 nssa-external
    1 nssa-external 2 route-map allanRM03
neighbor 2.3.4.5 activate
neighbor 2.3.4.5 route-map allanRM01 in
 neighbor 4.5.6.7 activate
 neighbor 4.5.6.7 route-map allanRM02 in
 default-information originate
 no auto-summary
 no synchronization
 exit-address-family
```

Source 2:

```
address-family ipv4 vrf VPN_PE_A
 redistribute ospf 10 vrf VPN_PE_A match internal external 1 external 2
 no auto-summary
 no synchronization
 exit-address-family
```

This creates two sources sections.

7 Now OpenManage Network Manager applies the regex in the criteria field to each of the sources. It returns *true* only if both sources pass (we selected the *Match All* radio button). In this case “Source 2" does not have those lines, so OpenManage Network Manager returns a false value.

8 The error details appear in the audit trail panel.

Regular Expressions

Regular expressions include metacharacters to instruct the program how to treat characters it encounters. These include the following: ^, $, . , | , { , } , [,] , (,), *, +, ? , \. If you want to match one of these metacharacters, you must prepend a backslash (\). So to match a literal question mark, rather than instructing regular expression matching to match 0 or 1 of a previous expression, you must enter \?.

The following table outlines standard, supported regular expressions.

Label	Pattern
Single digit	\d
Two digits	\d{2}
Three digits	\d{3}
Four digits	\d{4}
Five digits	\d{5}
Number	[0-9]+ One or more [0-9]* Zero or more
Decimal	.[0-9]+
Float	[0-9]+.[0-9]+
IP Address	(\d{1,3}.){3}\d{1,3}
IP Address/Mask	(\d{1,3}.){3}\d{1,3}/\d+
Domestic phone number with extension	1?[\s\-\/\.]*\(?([1-9]\d{2})\)?[\s\-\/\.]*([0-9]{3})[\s\-\/\.]*([09]{4})[\s\-\/\.x]*([0-9]{3,4})?
MAC Address	([0-9a-fA-F]{1,2}:){5}[0-9a-fA-F]{1,2}
MAC Address	([0-9a-fA-F]{1,2}.){5}[0-9a-fA-F]{1,2}
MIB2 OID	(1.3.6.1.6.1.2.1.(\d+\.)+\d)
Enterprise OID	(1.3.6.1.4.1.(\d+\.)+\d)
Time	[0-1][0-3]:[0-5][0-9]:[0-5][0-9]
All	.*
Ending Number	\d+$
Character	\w
Word	\w+ One or more. \w* Zero or more.
Whitespace	\s+One or more. \s* Zero or more.
String w/o space	\S+One or more. \S* Zero or more.
New Line	\n
FormFeed	\f

Label	Pattern
Tab	\t
Carriage Return	\r
Backspace	\b
Escape	\e
Backslash	\B
URL	(?:^|")(http|ftp|mailto):(?://)?(\w+(?:[\.:@]\w+)*?)(?:/|@)([^"\?]*?)(?:\?([^\?"]*?))?(?:$|")
HTML Tag	<(\w+)[^>]*?>(.*?)</\1>

Here are some examples of such expressions:

Label	Pattern
Email address (U.S.)	^[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,4}$
MAC Address	([0-9a-fA-F]{1,2}:){5}[0-9a-fA-F]{1,2}
Time hh:mm:ss	(0[0-9]|1[0-2]):[0-5][0-9]:[0-5][0-9]
IP Address	(\d{1,3}.){3}\d{1,3}
Validated IP Address (restricts what matches better than the previous example)	(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9?])\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9?])\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9?])\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)
MIB2 OID	(1.2.6.1.6.1.2.1.(\d+\.)+\d

The following are examples of the kinds of matching possible:

CAUTION:
Cutting and pasting from notepad into OpenManage Network Manager may cause carriage return or line-feed issues. Best practice is to compose these within OpenManage Network Manager.

Simple (CIsco ACL)

To match the following rows in a Cisco ACL:

```
access-list 159 permit icmp any any
access-list 159 permit tcp any any eq smtp
access-list 159 permit tcp any any eq www
```

To match these lines, simply create a compliance policy for *Config Term contains* (line contents) for each line.

Complex (Juniper)

When you have a multi-line statement to match, with varying elements, regular expressions are necessary. For example:

```
lab@MyServer# show protocols
bgp {
group internal {
type internal
export nhs
neighbor 10.1.1.1
}
```

```
}
```

In the above statement, the goal is to ensure an export policy in the BGP group internal called *nhs*. A suggested regex expression to match with the goal:

```
bgp/s+{/n/s+group/s+internal/s+{/n/s+type/s+internal;/n/s+export/s+nhs
```

NOTE:

Make sure you check Multi-line Support.

Another example:

```
lab@MyServer# show policy-options
policy-statement nhs {
term set-nhs {
then {
next-hop self;
}
}
}
```

The following regex statement matches this example:

```
policy-statement\s+ns\s+{\n\s+term\s+set-nhs\s+{\n\s+then\s+{\n\s+next-
    hop\s+self
```

Perl / Java (Groovy) Language Policies

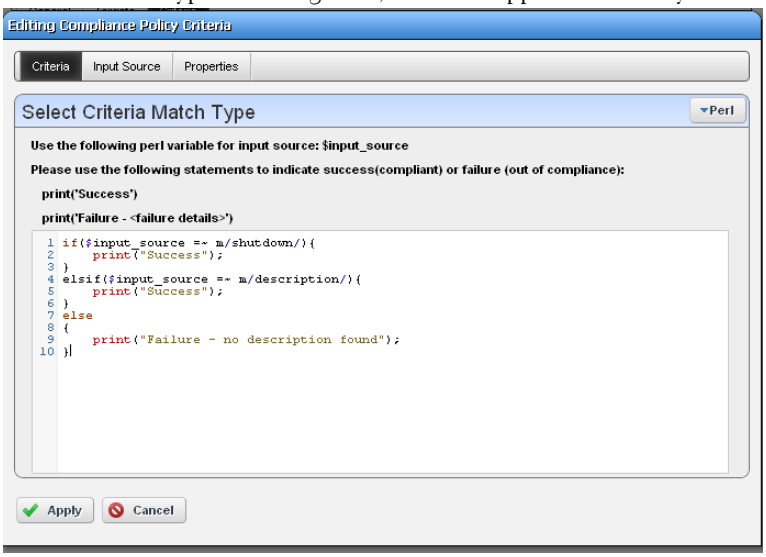
In addition to regular expressions, you can enter Config Terms that use either Perl or Java (Groovy) language capabilities for scans. The following sections describe these.

- Perl
- Java (Groovy)

These scans are compiled at runtime, and the Java scan uses the Groovy libraries, included with OpenManage Network Manager. You may need to install Perl on Windows application servers if you want to use that type of Config Term (it often comes with other supported operating systems). Refer to the *OpenManage Network Manager Installation Guide* for upgrading Perl instructions.

Perl

When you select Perl as the type of Config term, an editor appears that lets you enter Perl scans.



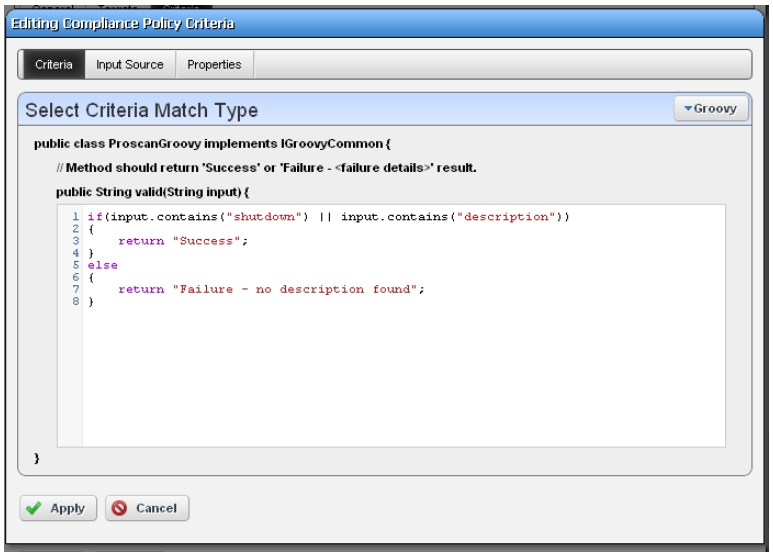
As the screen says `$input_source` is what the code scans. The following is example of the type of Perl you can enter that scans for contents like `description` in shut down interfaces, and prints output "Success" visible in the Audit viewer when it finds a matching term like `description` in whatever source you select:

```
if($input_source =~ m/shutdown/){
    print("Success");
}
elsif($input_source =~ m/description/){
    print("Success");
}
else
{
    print("Failure - no description found");
}
```

Notice that you can also combine these scans with the *Edit Source Group Criteria* regular expressions to streamline them.

Java (Groovy)

When you select Groovy as the type of Config term, an editor appears that lets you enter that type of scans.



As the screen says this implements ProScanGroovy or Groovy Java classes. The method should return 'Success or 'Failure -' results, and assumes `public String validate (String input) {` precedes what you enter in the text editor. The following is example of the type of Java code you can enter that scans for contents like `description` in shut down interfaces, and prints output "Success" visible in the Audit viewer when it finds a matching term like `description` in whatever source you select:

```
if(input.contains("shutdown") || input.contains("description"))
{
    return "Success";
}
else
{
    return "Failure - no description found";
}
```

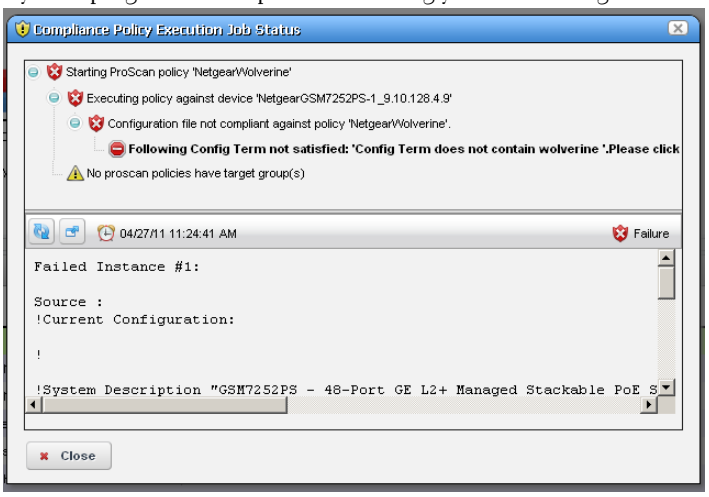
NOTICE

Notice that you can also combine these scans with the *Edit Source Group Criteria* regular expressions to streamline them.

Click *Save* to preserve the policy you have configured in these screens, or click *Close* (in the tool bar) to abandon your edits.

Compliance Policy Job Status

This screen displays the progress of compliance scanning you have configured.



You can the revisit history of this policy's use in the Audit portlet (see Audit Trail Portlet on page 630). Select an audit trail in this portlet to review details.

When you see the *Success* indicator, then the scanned item is compliant. If you also see a warning message that no policies have target groups, this does not have an impact on compliance.

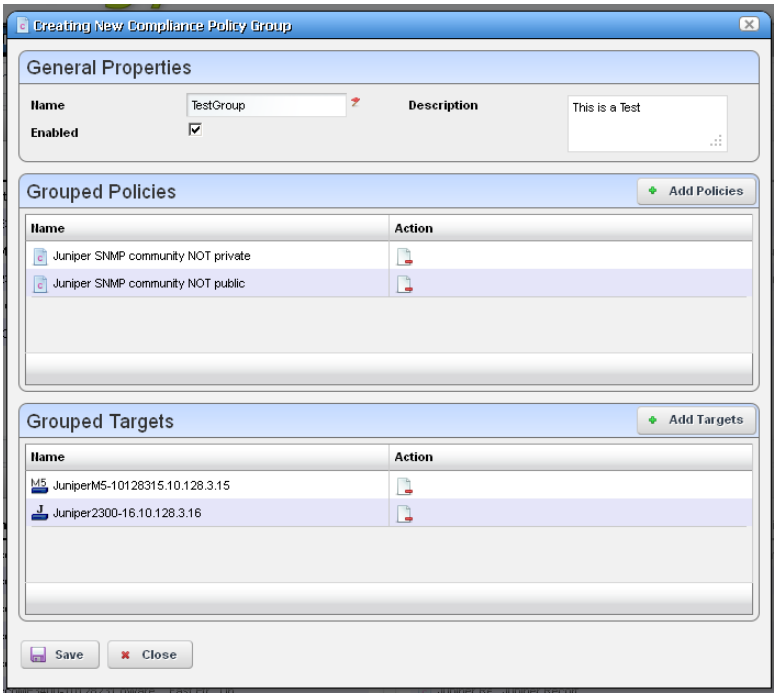
When you see the *Failure* indicator, then the scanned item is *Not* compliant. Select the "Following Config Term not satisfied" message to see the contents of the failed file at the bottom of this screen.

Executing Proscan policies may trigger a benign warning that "No proscan policies have target group(s)." You can safely ignore this warning message.

The advantage of selecting dynamic device groups is that newly discovered devices of the selected type automatically become members of the group, so ProScan scans them too.

Creating or Modifying ProScan Policy Groups

When you create or modify a ProScan Policy Group after right-clicking *New* > *Group* or *Open* when you have selected a group, the ProScan Policy Group editor appears.



This has the following to configure:

Name—A text identifier for the group.

Enabled—Check to enable this grouping.

Grouped Policies —Click *Add Policy* to select ProScan policies in a selector screen. Click the *Remove* icon to delete a selected policy. You can use individual policies in several groups. Individual policies that are part of groups display inherited group targets grayed out.

Grouped Targets—Click *Add Targets* to select targets for the scans.

Executing a group executes all the member policies and update the history records of the group and member policies. Any policy execution also update its parent group history records.

Standard Policies

Change Management comes with several policies and actions by default. These include ProScan policies and policy groups, as well as the corresponding Actions for correcting any violations, and Event Processing Rules that automate remedy actions. The following sections briefly describe a representative set of these (you may have more or less, depending on your package).

- Cisco Compliance Policies
- Cisco Compliance Actions

- Cisco Event Processing Rules

CAUTION:
Seeded Proscan policies are not necessarily correct by default. You must specify device targets at least. Given the variance in responses, particularly for Cisco devices, best practice is to test any such policy before you use it.

Cisco Compliance Policies

The following are Cisco Compliance policies included by default with your Change Management installation. Policies listed here are part of ProScan Policy Groups scanning for PCI, HIPPA, SOX, NSA, and CISP compliance. These appear at the bottom of this list.

COMPLIANCE Cisco Enable Secret—Use enable secret for enable level access to device; PCI 8.4

COMPLIANCE Cisco Finger Service (12.1+)—Disable Finger service; PCI 2.2.2

COMPLIANCE Cisco HTTP Server—HTTP server should not be running; PCI 2.2.2

COMPLIANCE Cisco Finger Service (11.3-12.0)—Disables finger service; PCI 2.2.2

COMPLIANCE Cisco Identd Service—Disable Identd service globally

COMPLIANCE Cisco Timestamps Logging—Use the timestamps service to show date and time on all log messages; PCI 10.2

COMPLIANCE Cisco Disable MOP—Disable MOP support on all Ethernet and VLAN interfaces; PCI.

COMPLIANCE Cisco NTP Redundant Servers—Ensures that more than one NTP server is defined; PCI 10.4

COMPLIANCE Cisco Disable NTP—Disable NTP if not in use; PCI 2.2

COMPLIANCE Cisco PAD Service—The packet assembler/disassembler (PAD) service supports X.25 links. This service is on by default, but it is only needed for devices using X.25; PCI 2.2.

COMPLIANCE Cisco Service Config—Disable autoloading of configuration files from a server; PCI 2.2.2

COMPLIANCE Cisco Password Encryption—The password-encryption service shows user passwords as encrypted strings within the configuration; PCI 8.4

COMPLIANCE Cisco IP Source Route—Disable handling of source routed packets.

COMPLIANCE Cisco SNMP RW Communities—Do not use SNMP Read-Write strings, and only use Read-Only strings with associated access lists; PCI 2.2.3.

COMPLIANCE Cisco TCP Small-Servers (11.2-)—Disables unneeded TCP services such as echo, discard, chargen, etc; PCI 2.2.2

COMPLIANCE Cisco TCP Small-Servers (11.3+)—Disables unneeded TCP services such as echo, discard, chargen, etc; PCI 2.2.2

COMPLIANCE Cisco UDP Small-Servers (11.2-)—Disables unneeded UDP services such as echo, discard, chargen, etc.; PCI 2.2.2.

COMPLIANCE Cisco UDP Small-Servers (11.3+)—Disables unneeded UDP services such as echo, discard, chargen, etc; PCI 2.2.2

COMPLIANCE Cisco VTY Exec Timeout—Set Exec Timeout on VTY ports; PCI 8.5.15

COMPLIANCE Cisco VTY Access Class Inbound—Set inbound access class on VTY ports; PCI 2.2.3.

COMPLIANCE Cisco VTY Login—Enable Login on VTY ports; PCI 2.2.3

COMPLIANCE Cisco VTY Transport Input Limit—Limit Input Transport on VTY ports; PCI 2.3

COMPLIANCE Cisco Set Login on Console Port—Enable login on console port; PCI 2.2.3

COMPLIANCE Cisco AAA Login—AAA login should be enabled; PCI 8.3

COMPLIANCE Cisco BOOTP Server—The BOOTSP server should be disabled; PCI 2.2.2

COMPLIANCE Cisco CDP Service—Disable CDP (Cisco Discovery Protocol) globally

COMPLIANCE Cisco Console Exec Timeout—Set an exec timeout console port; PCI 8.5.15

Cisco tacacs+ enabled

Cisco monitor logging Enabled

Cisco console logging Enabled

Cisco buffered logging Enabled

Cisco SNMP Community String NOT public

Cisco SNMP Community String NOT private

Cisco RADIUS Enabled

Cisco Interfaces MUST have Description

Cisco Banner Enabled

Cisco ACL RFC 1918 space

Cisco ACL Permit Transit Traffic

Cisco ACL Permit RIP

Cisco ACL Permit OSPF

Cisco ACL Permit IGRP

Cisco ACL Permit EIGRP

Cisco ACL Permit BGP

Cisco ACL Deny access to internal infrastructure

Cisco ACL BGP AS Source

Cisco ACL Anti Spoofing

Cisco ACL - Deny special use address source

Cisco session-timeout' Enabled - ALL LINES

Cisco exec-timeout' enabled ALL LINES

ProScan Policy Groups

The following combine the ProScan Policies described above into groups to scan for compliance.

PCI Compliance for Cisco—This includes the following COMPLIANCE policies: Cisco VTY Transport Input Limit, Cisco VTY Login, Cisco VTY Exec Timeout, Cisco VTY Access Class Inbound, Cisco SNMP RW Communities, Cisco Password Encryption, Cisco Finger Service (12.1+), Cisco Finger Service (11.3-12.0), Cisco Disable NTP, Cisco Identd Service, Cisco AAA Login, Cisco UDP Small-Servers (11.2-)

HIPPA Compliance for Cisco—A policy group. This includes the following COMPLIANCE policies: Cisco VTY Transport Input Limit, Cisco VTY Login, Cisco SNMP RW Communities, Cisco Set Login on Console Port, Cisco Password Encryption, Cisco PAD Service, Cisco HTTP Server, Cisco Enable Secret, Cisco Timestamps Logging, Cisco NTP Redundant Servers, Cisco Finger Service (11.3-12.0), Cisco Finger Service (12.1+), Cisco BOOTP Server, Cisco CDP Service.

SOX Compliance for Cisco—A policy group. This includes the following COMPLIANCE policies: Cisco VTY Login, Cisco VTY Transport Input Limit, Cisco SNMP RW Communities, Cisco Set Login on Console Port, Cisco Password Encryption, Cisco PAD Service, Cisco Finger Service (11.3-12.0), Cisco Finger Service (12.1+), Cisco HTTP Server, Cisco Identd Service, Cisco UDP Small-Servers (11.3+).

NSA Compliance for Cisco—A policy group. This includes the following COMPLIANCE policies: Cisco VTY Login, Cisco VTY Transport Input Limit, Cisco SNMP RW Communities, Cisco VTY Exec Timeout, Cisco Service Config, Cisco Password Encryption, Cisco PAD Service, Cisco HTTP Server, Cisco Finger Service (12.1+), Cisco Finger Service (11.3-12.0), Cisco Enable Secret, Cisco Disable MOP, Cisco Disable NTP, Cisco NTP Redundant Servers.

CISP Compliance for Cisco—A policy group. This includes the following COMPLIANCE policies: Cisco UDP Small-Servers (11.3+), Cisco VTY Transport Input Limit, Cisco VTY Login, Cisco VTY Exec Timeout, Cisco VTY Access Class Inbound, Cisco Password Encryption, Cisco Finger Service (12.1+), Cisco Finger Service (11.3-12.0), Cisco Enable Secret.

Cisco Compliance Actions

Remedial actions are often part of the process of change management. These may be triggered by the Cisco Event Processing Rules, and are included as part of the Standard Policies.

Compliance Cisco AAA Login—To avoid being locked out of the router, define username and password on the access server before starting the AAA configuration.

Compliance Cisco Finger Service—Disables the ip finger service.

Compliance Cisco HTTP Server—Disables http.

Compliance Cisco Identd Service—Disables identd

Compliance Cisco IP Source Route—Disables ip source route

Compliance Cisco UDP Small-Servers (11.3+)—Disables PCI UDP Small-Servers (11.3+).

Compliance Cisco TCP Small-Servers—Displace PCI Cisco TCP Small-Servers.

Compliance Cisco BOOTP Server—Disables PCI Cisco BOOTP Server.

Compliance Cisco PAD Service—Disables the PAD service.

Compliance Cisco Timestamps Logging—Enables PCI Cisco Timestamps Logging.

Compliance Cisco SNMP RW Communities—Removes RW community string with user input.

Compliance Cisco Password Encryption—Enables PCI Cisco Password Encryption.

Compliance Cisco CDP Service—Disables CDP Cisco Discovery Protocol.

COMPLIANCE Cisco VTY Transport Input Limit

COMPLIANCE Cisco VTY Login

COMPLIANCE Cisco VTY Exec Timeout

COMPLIANCE Cisco VTY Access Class Inbound

COMPLIANCE Cisco Set Login on Console Port

COMPLIANCE Cisco Service Config

COMPLIANCE Cisco SNMP RW Communities

COMPLIANCE Cisco Password Encryption

COMPLIANCE Cisco PAD Service

COMPLIANCE Cisco NTP Redundant Servers

COMPLIANCE Cisco Enable Secret

COMPLIANCE Cisco Disable NTP

COMPLIANCE Cisco Disable MOP

COMPLIANCE Cisco Console Exec Timeout

Cisco Event Processing Rules

The event processing rules here typically tie Cisco Compliance Policies with remedial Cisco Compliance Actions.

Compliance Cisco AAA Login Remediation—Triggers a task to configure an AAA login.

Compliance Cisco BOOTP Server—Corrects PCI Cisco BOOTP Server compliance failures.

Compliance Cisco CDP Service—Corrects PCI Cisco CDP Service compliance failures.

Compliance Cisco Finger Service—Corrects PCI Cisco Finger Service compliance failure.

Compliance Cisco HTTP Server—Corrects http server compliance failures.

Compliance Cisco Identd Service—Corrects PCI Cisco Identd Service compliance failures.

Compliance Cisco IP Source Route—Corrects PCI Cisco IP Source Route compliance failures.

Compliance Cisco PAD Service—Corrects PCI Cisco PAD Service compliance failures.

Compliance Cisco TCP Small-Servers—Corrects PCI Cisco TCP Small-Servers compliance failures.

Compliance Cisco Timestamps Logging—Corrects PCI Cisco Timestamps Logging compliance failures.

Compliance Cisco UDP Small-Servers (11.3+)—

Juniper Compliance Policies

Packages that support Juniper devices have the following policies:

Juniper FW Filter Private IP—RFC 1918

Juniper Policer DNS—Protect from source address spoofing

Juniper Policer NTP—Protect from source address spoofing

Juniper Policer RADIUS—Protect from source address spoofing

Juniper Policer SNMP—Protect from source address spoofing

Juniper Policer SSH—Protect from source address spoofing

Juniper Policer Small BW—Protect from source address spoofing

Juniper Policer TCP—Protect from source address spoofing

Juniper Recommended Logging—Confirms recommended logging is on.

Juniper SNMP community NOT public — Checks the SNMP community is not "public" closing a potential security hole.

Juniper SNMP community NOT private — Checks the SNMP community is not "private" closing a potential security hole.

Juniper ALL Services Policy—*Note:* this compliance policy will typically be modified per deployment.

Juniper Recommended SSH—Confirms recommended SSH is on.

Juniper Recommended Syslog—Confirms recommended syslogging is on.

Change Determination Process

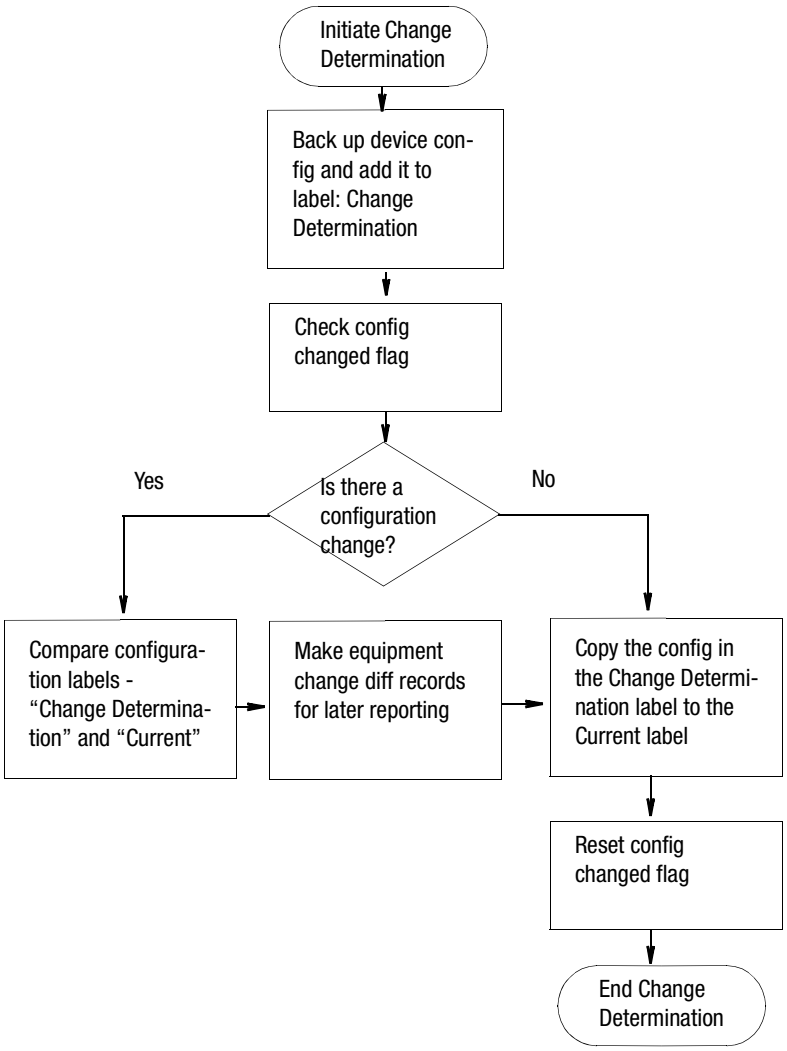
If you run the *Change Determination Process*, it collects all the configuration changes that occurred on the target resources since the last time this process ran. It also associates these changes with the date and time when the Change Determination process runs. After running Change Determination, you can then produce a report (see *Compliance and Change Reporting* on page 349), outlining all such changes by date and time. This report comes seeded with installation.

OpenManage Network Manager stores incremental changes as *RedcellConfigChangeRecords* by device/timestamp. The *ConfigChangeRecordsDAP* Database Aging Policy (DAP) manages how long the OpenManage Network Manager database retains these records. This DAP's default setting stores incremental records for 30 days, then archives or purges them. Reporting shows only records in the database; therefore, by default, the *Configuration Change Report* shows only resource changes made in the last 30 days, but no older. Change this default by changing the number of days to retain such records with the DAP.

The next section describes Change Determination Process Workflow.

Change Determination Process Workflow

Change Manager seeds Change Determination Process and ProScan group operations. You can configure this to run on groups of your choosing if you create a new Change Determination Process group operation.



This process records what is removed, updated or added since it last ran on a scanned device's configuration. If you run the Change Determination Process, it first backs up the devices' configuration(s), and stores those with the Change Determination label.

Change Determination Process then looks for Config Changed Flags, and if it finds such flags, indicating a change occurred on the device and/or Change Determination has not run on it, the process then compares the device's changed configuration (in the Change Determination label) to the one in the Current label, storing the difference for future reporting.

At its end, the Change Determination Process re-labels the configuration with the Change Determination label to the Current label, and it un-sets the Config Changed Flag on scanned resources so the flag will not signal change occurred when Change Determination runs again.

After running the Change Determination Process, you can run the Configuration Change report to display what changed for a defined period. The contents of that report depends on the report filter, and the specified period. This report lists changed attributes in the configurations.

Triggering Change Management and ProScan

To trigger the Change Management for a device, right-click it in the Managed Resources portlet and select *Change Management* > *Change Determination*. You can also schedule Change Determination to run repeatedly, on regular intervals in the Schedules portlet.

You can similarly trigger ProScan by right-clicking a device, and selecting *Change Management* > *Execute ProScan* or *Execute ProScan Policy*. The former execute all policies connected with the selected device, while the latter allows you to select policy (or policies) to run. Creating a ProScan Group, lets you run all ProScan policies for each device within the selected group, scanning groups even if they consist of devices from different vendors. In ProScan, you can scan device configurations (of specified labels) or Adaptive CLI command output. (See How to: Use ProScan / Change Management on page 321).



How To:
Run the Change Determination Process

The following describes an exercise for the Change Determination process based on manually running it. To run the process as a response to events devices must transmit traps to OpenManage Network Manager. The next sections describe using Change Determination in the following ways:

- Change Determination Confirmation
- Event/Trap-Based Change Determination

Change Determination Confirmation

The following steps confirm change determination is working.

1. Initialize the Change Determination Report and let it do a configuration backup. The first time this runs, OpenManage Network Manager creates no diffs. It just initializes the Change Determination label.
2. Edit a configuration to make a change. For example, make a change in a device you have discovered. One benign change is to add a contact or a description to an interface.
3. Restore it to the device.
4. Execute the Change Determination process on the device by right-clicking it in the Managed Resources Portlet, and selecting *Change Management* > *Change Determination*.

   This then backs up the device, compares the original and altered configurations, and writes the difference to report later (see How to: Report on Change Determination on page 349 for the steps to run the report to see such changes).

   Since we have initialized the report in step 1, the updated report shows the changes made to the config file.

5 Repeat step 2 through 5 if you like after you have made further changes.

NOTICE

Best practice in production is to schedule a recurring run for Change Determination in the Schedules portlet. Notice that you can also disseminate the report by e-mail, or view previous reports in the web client, as described in the Reports portion of this guide.

Event/Trap-Based Change Determination

The following steps to trigger Change Determination based on events received by OpenManage Network Manager. Your devices must transmit traps to the OpenManage Network Manager installation, and must emit traps when changes occur, or this does not work.

1 Back up the configuration file for a device you have discovered.

2 Make a change to that device with the Managed Resources editor, or from a Direct Access command line.

3 Such changes make the device emit an event that may have further consequences. For example, for Juniper devices, the Juniper JUNOS Configuration Changed event is a correlation event.

4 To provide a response (and to normalize the emitted event), create an automation rule that emits a `redcellEquipmentConfigChangeNotification` event when OpenManage Network Manager receives creates a event in response to events like the `jnxCmCfgChange` event that occurs when Juniper devices change.

5 Create a rule to respond to `redcellEquipmentConfigChangeNotification` by running the Change Determination process. You do not have to back up the configuration after the change. See How to: Create Event Processing Rules to Trigger Change Determination Process below.

6 To see the change itself, run the Change Determination Report (see Compliance and Change Reporting on page 349 and How to: Report on Change Determination on page 349). The report displays the changes made.

How To:

Create Event Processing Rules to Trigger Change Determination Process

This exercise creates an Event Processing rule that has Change Determination respond to an event. The steps to configure such an event processing rule are as follows:

1 Create a new event processing rule by right-clicking in Event Processing Rules > *New* > *Post Processing* rule in the Event Processing Rule portlet.

2 Enter the name in the field labeled *Name*. (Example: Update Config Change Flag)

3 Click *Next* to go to the *Filter* tab.

4 For the *Specify Events* panel, click on the *Add* button to select the event to which this rule responds. A selector listing available events appears.

NOTICE

Notice you can limit the selector's displayed events by entering text in the filter at the top of the selector screen.

5 In the selector, click the event definition (here: `redcellEquipmentConfigChangeNotification`), and confirm your selection.

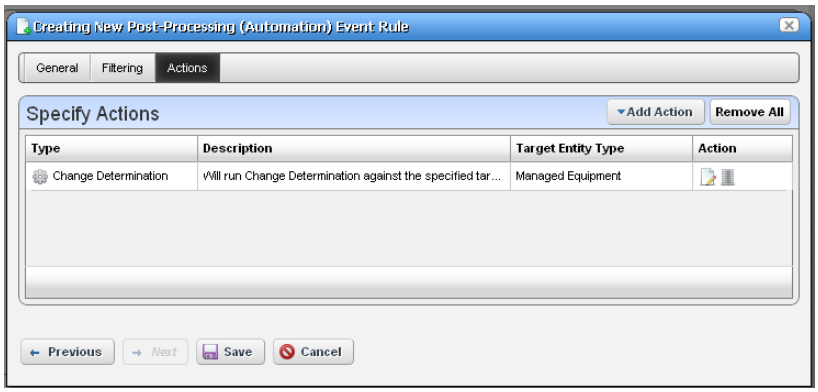
6 Click *Done* to accept the *Event(s)* you have configured.

7 Notice you can further filter which events this rule responds to with the lowest panel in this screen's *Filter Conditions* panel by clicking *Add Filter*. For example, you could create a rule that responds only to events from a particular IP address. For now, we will not configure additional filters.

8 Click *Next* to open the *Actions* tab.

9 Click *Add Action*, and click the *Custom* action alternative, then click Keyword Search and select Change Determination. That action appears in the drop-down combo box. Notice you can also select a target in the action selector. By not selecting one, we run change determination against all Managed Equipment.

10 Click *Apply* and view the Change Determination action listed in the Actions screen.



Notice that you can add more actions, and edit or delete existing ones with the icons to the right. Click *Apply* once you have selected Change Determination.

11 Click *Save* to preserve this event processing rule. The rule should now respond to the configured event, triggering the action you configured.

NOTE:

Backup and Change Determination automates backing up target devices.
Also: Change Determination's current default is to compare files even if the "Config Change" flag has not been modified.

Change Determination Defaults

By default, Change Determination can run against all devices without requiring the config change update flag be set or updated based on events tied to the Update Config Change Flag event processing rule/action.

To disable the manual run-ability of the Change Determination process, uncomment the property in `\owareapps\changemgmt\lib\cm.properties` (or add it to `\owareapps\installprops\lib\installed.properties`).

```
##############################################
# Change Determination Flag
# Allows system to be flagged to only run
# change determination against devices we
# have received Config Change Event for.
# Default Behavior is to run change determination
```

```
# for All targets (the same as setting the below property = false)
#com.dorado.changemgmt.change.determination.require.config.events=true
```

Compliance and Change Reporting

The Compliance Policy Violation report is seeded when you have ProScan / Change Management in OpenManage Network Manager. Inventory Compliance Attributes for reporting can also appear in report templates when you install ProScan. These report in-compliance or out-of-compliance, the last compliance date (when last compliant or not compliant), last config date (when configuration last changed), last checked date (when change was last determined).

You can also run the Change Determination Report that displays changes made to configurations.

See Generating a Report on page 131 for more about reporting capabilities.

The Change Determination Report report displays detected changes based on a configuration change flag set when OpenManage Network Manager detects a change made to the device. To successfully execute this report, you must enable a scheduled Change Determination Process. The process must run before the reports has any contents. To run the process, go to the Schedules portlet, and schedule that change determination process.

Reporting Limitations

The Configuration Change Report only reports on incremental configuration changes discovered in the CD process. Simply making changes to configurations and backing them up in OpenManage Network Manager does *not* ensure these appear in *Configuration Change Reports*. They appear in reports only after running the CD process.

The *Configuration Change Report* includes a Filter that you can alter at runtime. By default, the report filters on *Type* only. If you want more filter criteria—like device IP, and/or date ranges—you must edit the Report filter. To edit the filter, in the Reports manager, right click the *Configuration Change Report*, and select *Open*, then edit the filter in the *Filter* screen by selecting that node on the left.

NOTICE

A recommended best practice is to execute the CD process as an operation run against multiple resources following a scheduled group backup of these resources. If you run backups every day, the *Configuration Change Report* then shows the daily changes, until they are purged from the database.

The application stores the specifics of what changed for future reporting.

How To:

Report on Change Determination

Follow these steps to produce regular change determination reports:

1 First, insure the devices you want to scan are discovered, and send change notifications to the application server.

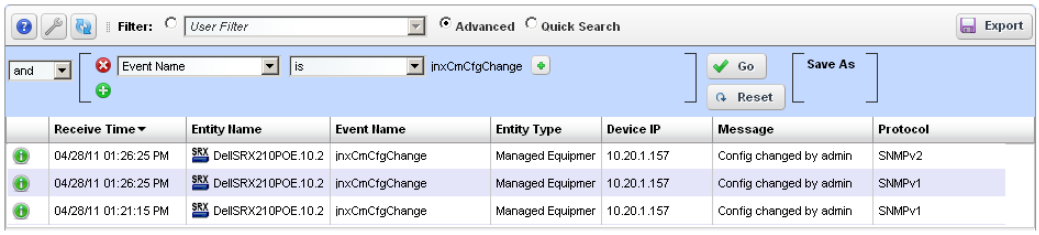
Juniper JUNOS-based routers, for one example, provide configuration change information with an SNMP trap. The following configuration determines that configuration change traps are being sent to a host 192.168.1.24:

```
trap-group test {
        categories {
            configuration;
```

```
        }
        targets {
            192.168.1.24;
        }
    }
```

Check your vendor's manuals to determine how to forward configuration change information to OpenManage Network Manager for your system. See Forwarding Configuration Change Commands on page 350 for others.

2 When OpenManage Network Manager receives a configuration change notification, in the JUNOS-based example, the device transmits an event (jnxCmCfgChange) to the OpenManage Network Manager mediation server. When received, this event automatically generates an event called OpenManage Network ManagerEquipmentConfigChangeNotification. Event history displays that notification.



3 When OpenManage Network Manager receives the OpenManage Network ManagerEquipmentConfigChangeNotification event, it can initiate (if enabled) an event processing rule called *Configuration Change*.

This processing rule triggers a flag in the OpenManage Network Manager database saying a change has occurred in the device's configuration and that OpenManage Network Manager should run change determination against the device when requested.

4 When you run OpenManage Network Manager's change determination process, it reviews the flag setting in the database and backs up a managed device if the flag indicates a change. This backup updates the OpenManage Network Manager system label *Current* which is then compared to the OpenManage Network Manager system *Change Determination* label. OpenManage Network Manager then writes the differences between the two labelled configurations to its database, where it is available for reporting purposes.

5 Once this occurs, the *Change Determination* label moves to point to the same configuration which is reflected by the *Current* label.

6 The report which can run to display these changes is OpenManage Network Manager's *Configuration Change Report*. It displays the name of the device in question, the IP address, date/time of change, who made the change, what was removed and what was added. You can schedule this report to run immediately after an Change Determination process too, so you can capture a history of changes.

Forwarding Configuration Change Commands

The following are setup commands for various other devices

Cisco

The following is the configuration to forward notifications to 192.168.1.176;

```
logging facility local0
```

```
logging 192.168.1.176
```

This configuration comes from executing the following commands on the CLI once you are logged in to privileged mode

```
conf t
logging on
logging 192.168.1.176
logging facility local0
end
wr mem
```

12

Serving Multiple Customer Accounts

Multitenancy lets you manage your customers' tenant networks from a central OpenManage Network Manager system while at the same time providing them with secure access to their specific resources. OpenManage Network Manager does this with a two-tiered customer multitenant service provider (MSP) model, assigning each customer a specific security domain for their specific resources. OpenManage Network Manager then restricts access to the domain to the customer or a member of the MSP domain See also Multitenant Batch Imports in the next section.

Multitenancy is a OpenManage Network Manager extension.

Multitenant Batch Imports

You can import Discovery Profiles, Authentications and Contacts to target multitenant domains with a command line importer. The command is `import[item]`, for example `importprofiles`, and these commands are in the `owareapps/redcell/bin` directory. These commands take the import file name as an argument. The required domains should exist in the OpenManage Network Manager system before import occurs. Import authentications before importing discovery profiles that refer to them. Example XML files with the `<customer>` tag for domains are in `owareapps/redcell/db`.

Configuring Chat for Multitenancy

Sometimes you may see Colleagues not members of a tenant site in the tenant site's status bar. This is not necessary. To change this so only tenant site personnel appear in the Colleagues panel, do the following:

1. In Control Panel, under *Portal* > *Users and Organizations*, click the link under *Name* to the tenant site.
2. With the *Actions* button in the relevant User's field, select *Edit*.
3. In the *Sites* panel (the link is on the right), remove OpenManage Network Manager, and any other sites present, except the tenant site itself. Only the tenant site remains as the source of chat colleagues who appear in the status bar.
4. Go to the tenant site. You should only be able to see authorized users for the tenant site who are on the tenant site. If you are on the master site, then you can still see all users.

Configuring Multitenancy, Site Management and Access Profiles

OpenManage Network Manager can support multiple client organizations from a single instance. It can also constrain data access for logged on users depending on the client organization to which they belong. To implement multitenancy, follow the How to: Create a Multitenancy Environment on page 355 below.

To understand the data constraints on tenants within a Multitenant OpenManage Network Manager environment, see Constraining Data Access on page 368. See also User Site Access on page 366 for how to give users access to multiple tenant sites.

The following diagram describes the relationship between the pieces of Multitenancy in the order needed to configure a tenant site. See it in narrative form in How to: Create a Multitenancy Environment on page 355

Multitenancy Components

Control Panel
(Multi-Page) Site Template
Page Template
→ Action > View Page to add / arrange portlets on these templates

Site Management Portlet
Create Tenant Site

(Must assign previously-created Site or Page Template while creating the new site for the first time)

Access Profile Templates Portlet
Create Access Profile Templates

(Can configure OpenManage Network Manager capabilities for groups of sites)

Site Management Portlet
Configure Tenant Site Access Profile

(Right-click for AP Editor / AP Template Editor. Assign an Access Profile Template to be logically ANDed with the site's own Access Profile.)

Managed Resources Portlet
Right-click to assign devices to Tenant sites. See View and Further Configure Devices for the Site on page 356.

User Site Access Portlet
You can optionally configure multi-site access for selected users. See Configure User Site Access on page 356.

Discovery Profiles Portlet
You can optionally assign a discovery profile to a tenant site. See Assigning Sites in Discovery on page 357.

Provisioning Site-Creating User Permissions

The user(s) allowed to create tenant sites with Site Templates and the other features documented here are typically Administrators. However, if you want to allow another User like *Tenant Admin* to make tenant sites, you must grant that user's Role permissions in two areas within Control Panel:

Redcell > Permission Manager

Click the edit button to the right of the assigned Role, and grant the MSP-related permissions found (*MSP Access Profile Templates* and *MSP Site Management*). Search *All* permissions with the magnifying glass at the bottom of the editor to find these permissions.

Portal > Roles

Grant the selected user's Role permissions within this panel. Click the Role itself, then click the *Define Permissions* panel in the editor. Within the drop-down list, under *Site Content*, grant *Site Template* permissions if you want the user to create templates, and under *Portal*, grant *Sites* > *Site* and *Sites* > *Site Pages Variation* permissions configured as appropriate.



How To:

Create a Multitenancy Environment

Creating a Site Template

1. A tenant's website or portal is based on a Site or Page Templates you have created. See How to: Make A Site Template on page 360. Also, see Click "+ Add page" on the grey bar in the middle of the screen, fill in data and click Add page at the bottom on page 362 for instructions about creating them.
2. Right-click in the Site Management Portlet to create a tenant site. Click *Add Site* and the editor appears (see Site Management Editor on page 363).
3. While the Site Management Editor is still open, assign a Site or Page Template you have already created (see Portal > Site Templates on page 360 and Click "+ Add page" on the grey bar in the middle of the screen, fill in data and click Add page at the bottom on page 362). This creates the default website for the customer. You can only do this when creating the customer, you cannot do it after the customer is created.

△ CAUTION:

Deleting a Page Template already in use makes the page unusable. Don't do it! Also: A Site Admin can choose to hide some of a tenant site's pages from a Site Member through page permissions. The page permissions do not work, however, if the tenant site comes from a site template.

4. *Save* the tenant site.
5. If you want to configure the site further, click *Action* > *View Pages* in site as it appears in the list of tenant sites. You can add portlets, and they will become part of that site.

NOTICE

The Site Map portlet discloses a site's available pages and the portlets configured to be on each page. By default, the Site Map portlet is available from the Settings page by selecting the Site Map menu option. **Also**: Sites appear in the Control Panel under *Top Level Organizations*, along with the number of assigned users.

Creating an Access Profile Template

6 Access Profile Templates configure tenant site access to various capabilities. These templates provide an easy way to grant levels of access to resources (for example: *bronze*, *silver*, *gold*) to your customer base too.

Optionally, create an Access Profile Template, using the Access Profile Templates portlet described below. Right-click and select *New* in the Access Profile Templates portlet to create a template (see AP Editor / AP Template Editor on page 365).

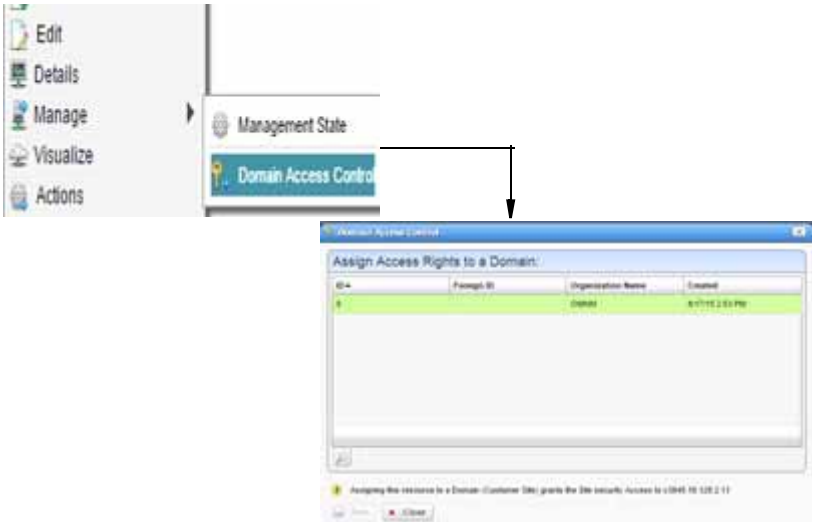
To create an individual site's Access Profile, right-click the tenant site you created in the Site Management portlet and select *Access Profile* from the menu. Notice you can select from available Access Profile Templates at the top of this screen too.

Every customer automatically has an Access profile which consists of any selected Access Profile Template and any customer-specific Access Profile you configure. Configure the Customer Resource Assignments by clicking *Add* in the Access Profile Editor. OpenManage Network Manager logically ANDs these with any selected template.

View and Further Configure Devices for the Site

7 To see the tenant website, right click the tenant site in Site Management, and select *Go to Site*. The tenant website opens, and you will see all the pages you configured when Creating a Site Template.

8 If you want to confine discovered devices to a particular tenant site, right-click them in the master site's Managed Resources. Right-click a device and select Manage > Domain Access Control to see the menu of available tenant sites.



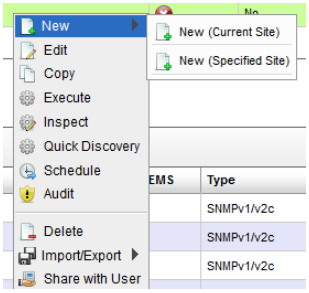
By default, only devices either discovered for an assigned site, or those explicitly assigned with this procedure appear in tenant sites.

Configure User Site Access

9 You can optionally assign specific users access to multiple tenant sites. See How to:Configure User Site Access on page 367 for step-by-step instructions.

Assigning Sites in Discovery

To create discovery profiles for a particular site, select the site in the *New (Specified Site)* action within the Discovery Profile portlet.



These devices are visible in the master site, but are assigned, by default, to the selected tenant site. Other tenant sites do not see them.

Supported Portlets

Multitenancy-supported portlets include the following:

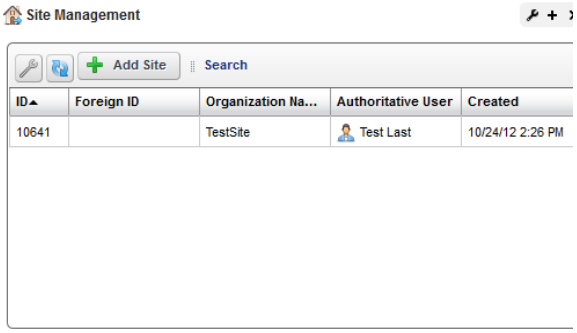
- Resources (including Ports, Interfaces)
- Customers
- Contacts
- Discovery Profiles
- Authentication
- Location
- Audit
- Alarms
- Event History
- Schedules
- Container View / Manager
- Map View
- Visualizer
- Dashboard Views[1]
- Reports
- Report Templates
- Actions
- Event Processing Rules
- Links - but only if the portlet is on the same page as resources
- Top N Portlets (not the RTFA Portlets though) / Top Problem Nodes
- Dashboard Views
- Audit Trails

If a portlet does not appear on this list, it does not support Multitenancy.

1. You must make a dashboard for performance monitoring on the tenant site if you want it to appear on the tenant site. Reconfiguring monitors makes dashboards misbehave on tenant sites,

Site Management

This portlet configures customer sites and organizations, including an administrative user for customer sites who can configure additional user accounts within the site. Optionally an organization can have its own website customize-able with non-standard graphics.



NOTE:

Rather than the contents management tasks typical for other portlets, the wrench icon in this portlet opens managing restrictions for those logging into the Multitenant environment. See Login Restrictions on page 359 for more about how those work.

The search function can locate a site based on the *Organization Name*, *Foreign Id*, *Authorized User* or the *ID*. This portlet offers the following options:

Add Site—Click the *Add Site* button at the top of the portlet to create a new profile. This opens the Site Management Editor with a few more options than you might see if you right click to *Edit* an existing profile.

After you have created a site, you can see the following in its right-click menu:

Edit—Edit an existing Profile with the Site Management Editor.

Access Profile—Opens the AP Editor, described in AP Editor / AP Template Editor on page 365. Use the selection pick list at the top of the editor to associate an Access Profile Template with the selected site.

To make the Access Profile customer or organization-specific, you can augment the permitted functionality in the selected template by adding shareable resources. Click the *Add* button.

Existing permissions from any selected Access Profile Template do not appear in the permission type totals on the left, nor are they eliminated from the available permissions that appear after you click *Add*.

A Site Admin can choose to hide some of a tenant site's pages from a Site Member through page permissions. The page permissions do not work, however, if the tenant site comes from a site template.

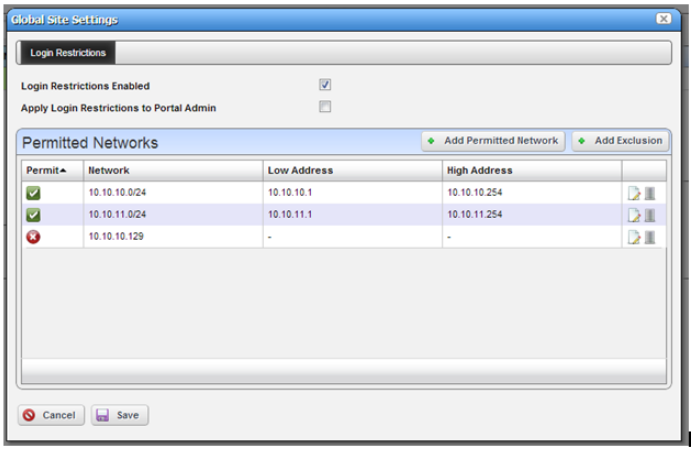
Go to Site [New Window/Tab]—Opens the Customer's site in a new window or tab in your browser.

Delete—Deletes the selected customer.

The expanded and summary portlets are the same. Columns in both include an automatically-provided *ID* for each customer, the *Organization Name*, *Authoritative User* (the administrator for the customer or organization), and *Created* which records the date the customer organization was created. See Portal > Sites / Site Templates in Control Panel below for more about site management capabilities.

Login Restrictions

The site management portlet lets you restrict access to configured network domains. Select the configuration icon (the wrench) which opens the Global Site Settings dialog.



Here the administrator can add networks that the primary site's central domain users can login from, or exclusions of things like a proxy server within one of the permitted networks which allows external access to the web server. When attempting to login from an IP address other than those permitted a message appears saying *Login is restricted from your current IP [IP Address]*.

Notice that you must check *Login Restrictions Enabled* to begin restricting access. When you check that, global portal users can only log in from defined, permitted networks. You can also elect to *Apply Login Restrictions to Portal Admin* with that checkbox, too.

Portal > Sites / Site Templates in Control Panel

In addition to the Site Management portlet, authorized users can manage sites from the Control Panel. See the following:

- Portal > Sites
- Portal > Site Templates
- Click "+ Add page" on the grey bar in the middle of the screen, fill in data and click Add page at the bottom

△ CAUTION:
Site creation must occur through OpenManage Network Manager's Site Management portlet. If you bypass this portlet you will not create all the data that let OpenManage Network Manager manage the sites.

Portal > Sites

A list of sites created in Site Management Editor appears in this screen, and clicking the *Actions* button to the right of the listed site lets you manage the page configuration and user membership for tenant sites as well as the main site, if your login is a user authorized to access the main site.

Click the link that names a site to see its logo appear on the Control Panel page, and to select any site template (the template selected for Public Pages also appears for Private Pages). You can even check *Enable propagation of changes from the site template* to propagate changes from that template to the site itself.

You can also *Deactivate* or *Delete* a site listed there. These functions supplement the Site Management portlet and Site Management Editor described in this document.

Portal > Site Templates

Multitenancy uses Site Templates configured in Control Panel to configure new tenant sites. You can select a Site Template or Page Template when you create a new tenant site. The following describes how to create a new Site Template.



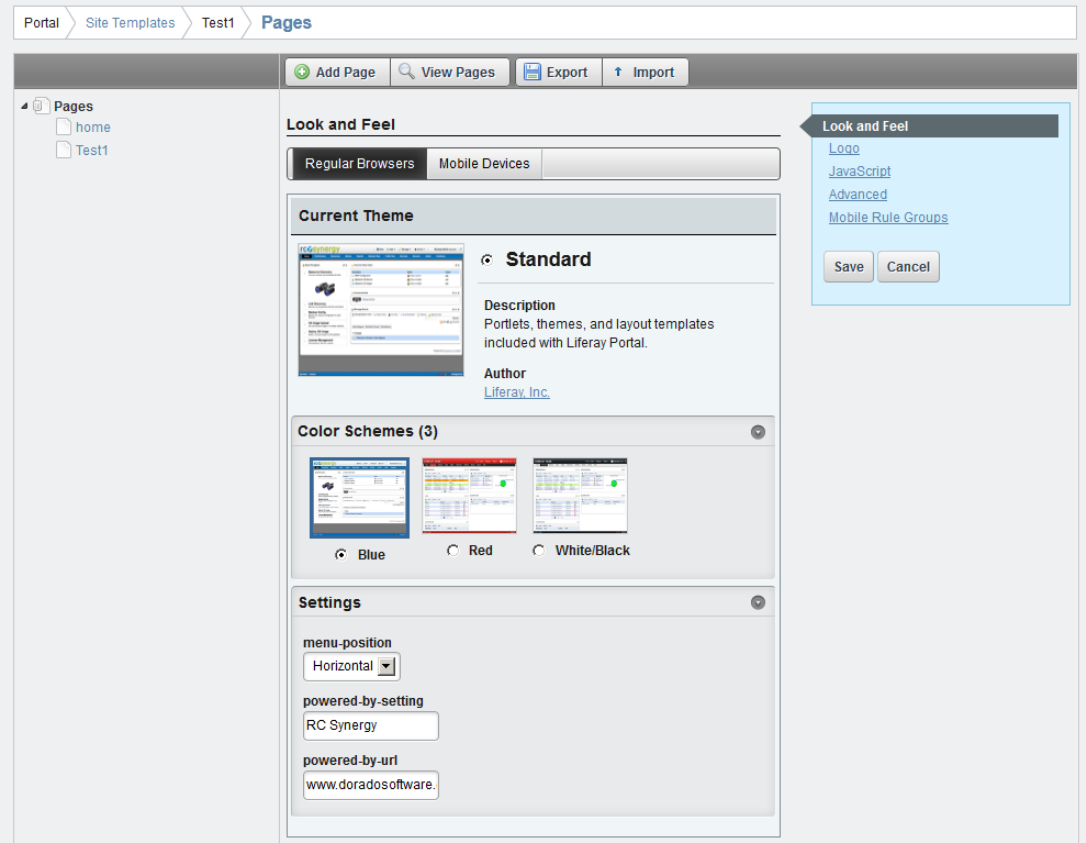
How To:

Make A Site Template

1. Navigate to Control Panel
2. Click the *Portal* > *Site Templates* link.
3. Click *Add* to create a new site template. Notice that, in addition to configuring the Site Template's Name and Description, you can check to make a template *Active*, and to *Allow Site Administrators to Modify the Pages Associated with this Site Template* at the bottom of the *New* screen.
4. *Save* the new template.
5. Click the *Actions* button to the right of listed templates to *Edit*, *Manage Pages*, *View Pages*, configure portal *Permissions*, or *Delete* a selected template.

   The *Permissions* configurable here are for the portal, not OpenManage Network Manager, permissions. Use Portal > Roles to configure those. See Access Profile Templates on page 364 for more about configuring them on multitenant types.

6 Click *Manage Pages* to see the tenant site's page setup in tree form on the left, and more editor options on the right and center (for example, alter the look and feel, *Logo* and so on)[



7 Click *Add Page* to create a new page. By default, new pages appear below the root node on the tree at the left, but you can drag and drop them to any new location.

8 After you configure the page layout(s) as you like, including the Logo, and color scheme, you can preview them by clicking the *View Pages* button at the top of the editor screen. This opens the new configuration in a new browser tab.

9 To configure portlets on these pages, simply use the *Add* > *Applications* menu item. When you re-open the Site Template, the portlets appear as you have configured them.

10 Notice that you can also *Import* a variety of settings from an exported LAR file with the button at the top right of the screen if you want pages that nearly duplicate each other. Notice also that you can *Export* / *Import* these Site Templates with the buttons at the top of the editor.

11 Click a page in the tree on the left to expose editing capabilities for that page, including its *Look and Feel* and *Layout* (columns) with links that appear on the right. Notice that you can also *Copy Portlets from Page* to copy the portlet setup from an already-configured page in this Site Template.

How To:
Add a new vertical menu page

1 Go to control panel > OMNM menu section > Site pages

2 Click "+ Add page" on the grey bar in the middle of the screen, fill in data and click Add page at the bottom

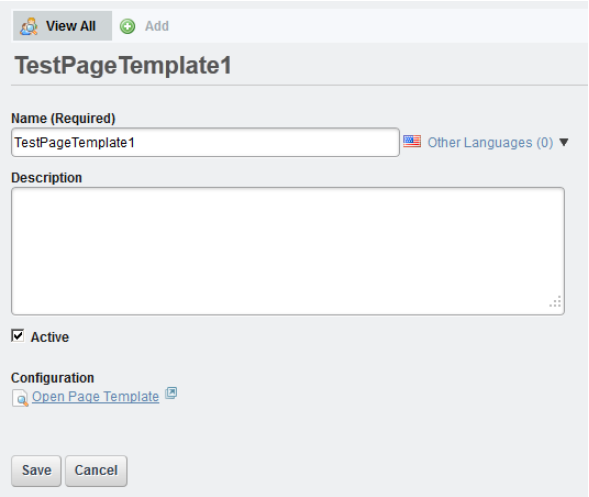
3 Page is added at the bottom of the displayed Private Pages hierarchy tree. Drag the menu item to a desired location if necessary.

4 Click save in the details panel on left.

The page is now added in the vertical menu.

Portal > Page Templates

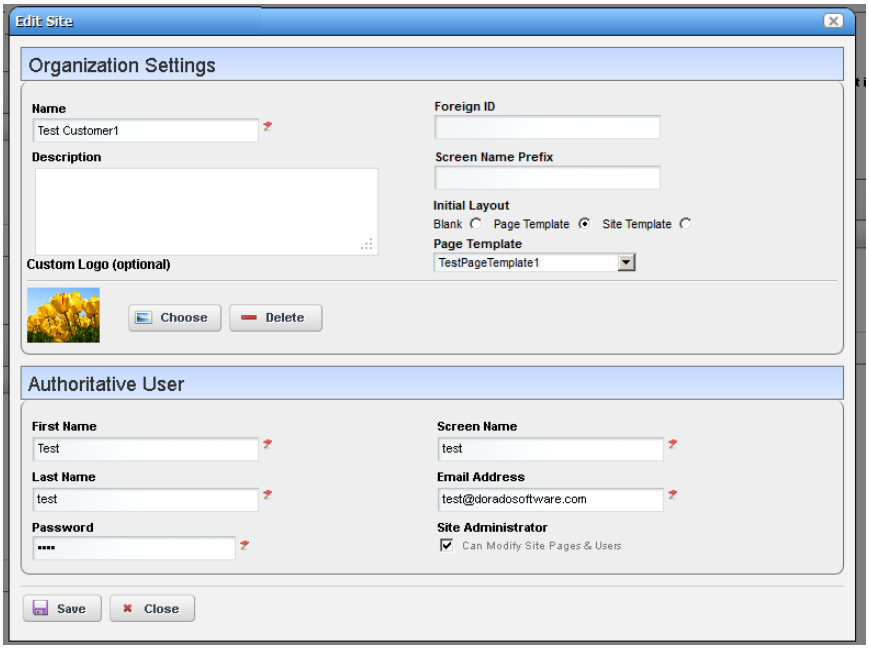
This lets you edit a single page template as you would several pages in Portal > Site Templates.



Click the *Open Page Template* link at the bottom of this screen to see the page in a separate tab or window, and add the desired portlets.

Site Management Editor

This editor lets you configure customers, site administrators and their organizations.



It has the following fields and labels:

Organization Settings

Name—A unique name for the customer's organization.

Foreign ID—An optional identifier for the customer's organization.

Screen Name Prefix—Enter a screen prefix for the customer. The prefix must be unique within the system.The prefix is prepended to all user accounts to insure no accounts conflict across organizations. So if you create a customer with a prefix of DS, and his screen name is Mark then the user's login is DS-Mark. This is automated in Site Management Editor, but you must manually enter the prefix for users created in Control Panel.

By default this field is required. If you do not want to use screen name prefixes then edit the `oware/synergy/conf/server-overrides.properties` file and uncomment the following property:

```
#site.screen.name.prefix.required=false
```

Description—Any text description for this customer.

Custom Logo (optional)—Select a graphic. The subsequent selection screen lets you select a file, and recommends it be transparent, 50 pixels in height, and proportional in width. Once you have successfully selected and uploaded a logo, a preview appears below this label.

Initial Layout—Select from the radio buttons. This determines the configuration for the initial screen provisioned for the customer's site. See Portal > Site Templates on page 360 and Click "+ Add page" on the grey bar in the middle of the screen, fill in data and click Add page at the bottom on page 362 for instructions about configuring these. To take effect, these must exist before the Customer exists.

Authoritative User

These fields configure the tenant site's administrator. The user information entered here automatically configures a user in OpenManage Network Manager.

First / Last Name—The name of the administrator.

Screen Name—The screen name of the administrator.

Email Address—The e-mail address of the administrator.

Password—The administrator's password.

Site Administrator—This grants the user site administration privileges. These privileges let administrators add or remove users within the site, and configure pages and layouts.

When an organization's administrator assigns permissions to their users and/or user groups they are constrained by their own access permissions granted by the Multitenant site provider, ensuring that such administrators cannot grant more permissions then they have. See How to:Configure User Site Access on page 367 for information about granting users access to more than one site.

When you try to log in as a multitenant user, even if you do not type it as part of the login ID, OpenManage Network Manager automatically prepends the Screen Name Prefix if you create the user in the Site Management Editor. If you make other users for the tenant site manually in Control Panel, you must manually add the prefix to assign them to the correct site. In either case, you must type that prefix as part of the login ID.

Click *Save* to preserve your edits, or *Close* to abandon them.

Access Profile Templates

Configure data access for Multitenant Service Providers (MSPs) through an Access Profile (AP), configured in these portlets as described in AP Editor / AP Template Editor on page 365, or more accurately, in that AP Template plus whatever customization you configure for Site Management when you assign it an AP.

An AP describes which entities within the system a site can access. When enforcing AP-based access, OpenManage Network Manager identifies applicable entities based upon the Site ID. The fundamental difference between this approach and Site ID filtering is its ability to access an entity from multiple sites. For example multiple customer sites can have access to an AP template.

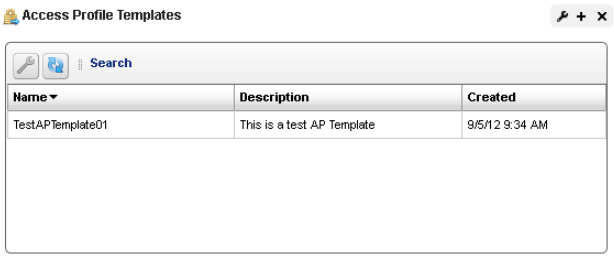
This approach, along with functional permissions, lets MSPs control exactly what their customers can do and see.

For example, an MSP offers Gold, Silver and Bronze tiers of service. At the Gold level customers have access to 12 pre-defined reports and they can create their own reports from existing report templates. At the Silver level customers can only access the 12 per-defined reports and at Bronze level the customer can only access three reports, a subset of the 12.

To do this within OpenManage Network Manager, the MSP would first create the necessary report templates and report definitions. Assume there are eight templates and 12 report definitions. At the Gold level the MSP would provide access to the eight templates and the 12 report definitions. The MSP could also give gold customers the functional permission to create a report definition. At the Silver level the MSP gives the customer access to the 12 reports but no functional permission to create new reports. Since customer at the silver tier cannot create report definitions they also

cannot access report templates. Finally at the Bronze level the MSP provides access to the three specific reports available at that service level. In all cases, only target devices assigned to the respective sites appear in the report(s).

This portlet lets you configure the kind of access available to customers configured in the Site Management portlet.



This displays a profile's *Name*, *Description*, and *Created* date by default. You can also add a column to display its *Updated* date. The expanded portlet displays the same columns and a Reference Tree snap-in showing connections to the selected Profile.

This portlet's right-click menu has the following items:

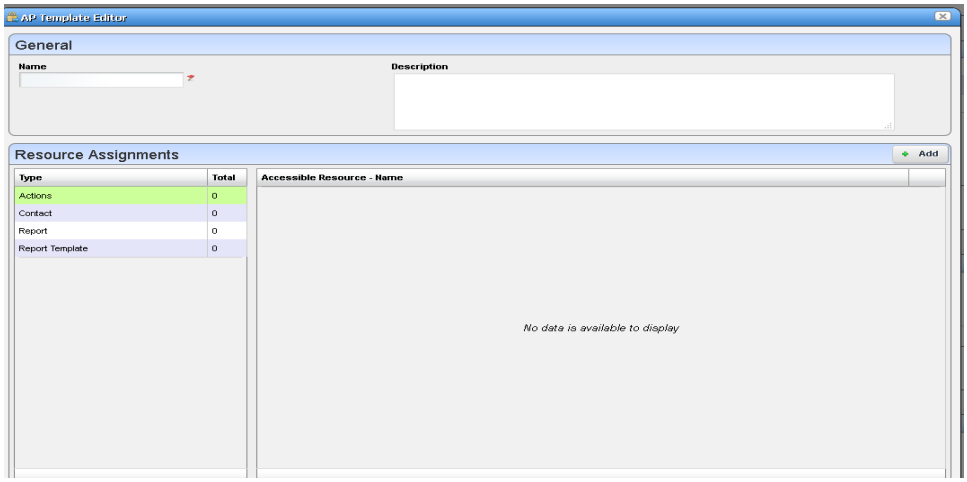
New / Edit—Create a new or edit an existing template with the AP Editor / AP Template Editor. Create Access Profiles when you assign them to sites by right-clicking in the Site Management portlet.

Delete—Remove a selected profile.

AP Editor / AP Template Editor

These editors let you create and modify Access Profiles for single sites and Templates that may apply to several sites. To standardize access profiles across multiple customers, create a template. Right-click a site in the Site Management portlet to see the Access Profile Editor, where you can select templates. Right-click in the Access Profile Templates portlet and select *New* to create a template.

These profiles configure access to OpenManage Network Manager resources for customers configured in the Site Management portlet. Use that portlet's right-click menu to associate Profiles with Customers.



The editor screen contains the following fields:

Template Association

This pick list contains the templates previously configured in Access Profile Templates portlet. This Template Association panel does not appear in the AP Template Editor.

General

Name—An identifier for the Access Profile.

Description—A text description for this Profile.

Resource Assignments

This panel displays the Type of resource on the left. To select resources of that Type, click to select it, then click the *Add* button over the right panel. A selector of available types of access to resources appears. Select the desired ones for the Profile, and they appear listed below the *Add* button. Use the icon to the right of the permission to remove it from a profile. The types of resources constrained by these templates include the following:

- Actions
- Contacts
- Reports
- Report Templates

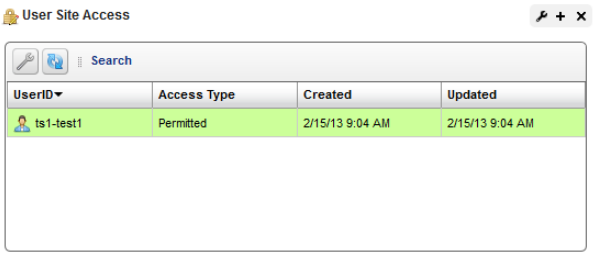
Click *Save* to preserve your edits, or *Close* to abandon them.

The access permissions configured here dictate what users can do, and can further be limited by OpenManage Network Manager's functional permissions.

This AP applies to users created in the base domain as well as those created within an organization. Those capabilities include assigning permissions directly to an individual user or to a user group. Any user within the group inherits group-assigned permissions.

User Site Access

By default, users can access only one Multitenant site. If your network has users who need to see more than one site, you can configure such User Site Access in this portlet.



Right-clicking in this portlet offers the following menu items:

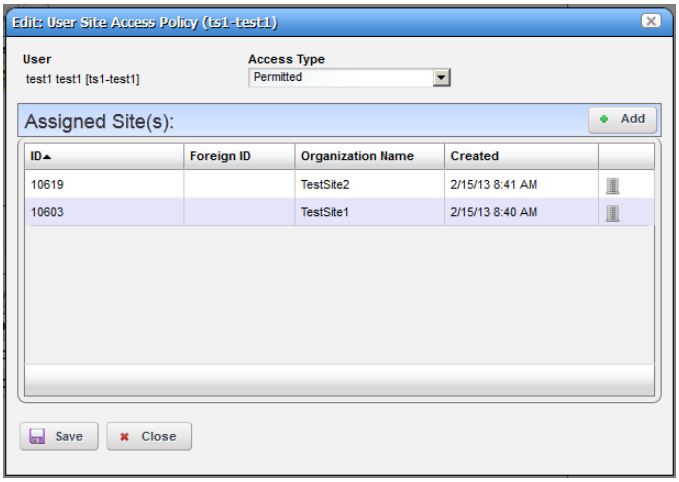
New—Create a new mapping of a user to a set of sites. When you click this, a screen appears where you can select a user already configured in the system. The User Site Access Policy editor appears after you have selected a user. Configure site access in that editor.

Edit—This opens the User Site Access Policy editor for the selected, already configured UserID. Editing existing policy may take up to 10 minutes to take effect. If user wish to see the effect right away, delete and recreate the policy.

Delete—Delete the user site access configuration selected.

User Site Access Policy

This editor assigns Multitenant sites to users.



This screen offers the following selections for User Site Access:

Access Type—Select from *Permitted* (allow access to the listed sites) or *Restricted* (deny access to the listed sites).

Assigned Site(s)—Click *Add* to select sites for the selected user's access / restriction. Click the icon on the right of a listed site to delete it.

Click *Save* to preserve a User Site Access Policy, or *Close* to abandon your edits.

How To:

Configure User Site Access

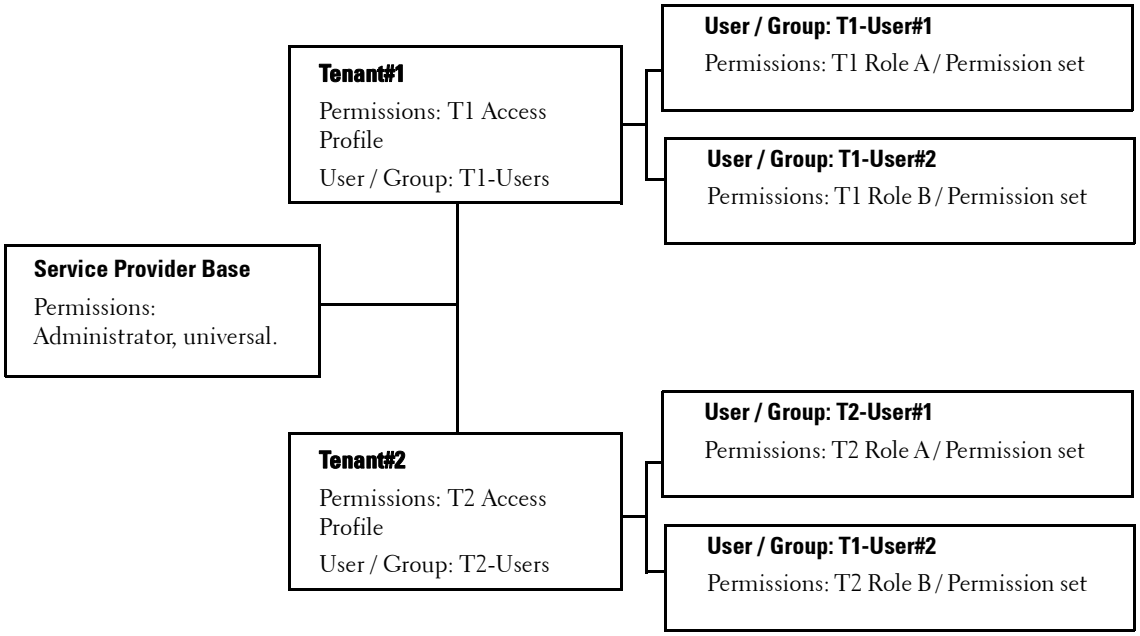
Follow these steps to configure User Site Access:

1. If you have not previously configured Multitenant sites, you must do so before configuring User Site Access. See How to:Create a Multitenancy Environment on page 355 for step-by-step instructions about how to do that.
2. Create any user(s) for whom you want to configure access.
3. Configure those user(s) permissions. See Configure Resource Level Permissions in this guide.
4. Right-click in the User Site Access portlet and select *New*.
5. In the subsequent screen, select the user whose Multitenant site access you want to configure.
6. The User Site Access Policy editor appears.
7. In the *Access Type* pick list, select whether you want to grant the selected user access to the sites you pick (*Permitted*), or you want to deny their access to the sites you select (*Restricted*).
8. Click the *Add* button with the green plus.
9. In the subsequent screen, select the site(s) your user can access or from which your user is to be excluded.

10 Click *Save*. The user you have configured should have access to (or be restricted from) the Multitenant sites you have configured.

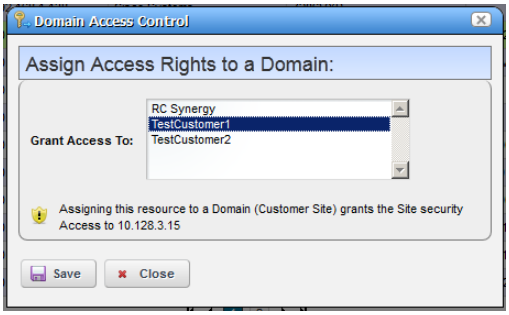
Constraining Data Access

Constraining data access for a site involves two primary mechanisms: Site ID Filtering, also referred to as Domain Id filtering, and the kind of filtering provided by Access Profile Templates. The following diagrams how multitenancy can work.



Manage > Domain Access [Resources]

If you right-click a Managed Resource, you can select Manage > Domain Access to configure different tenant domains' access to the selected device.



Click the domain(s) (besides the master domain) where you want to have access to the device and then click *Save*.

Site ID Filtering

Site Management / organization site include an internal identifier. OpenManage Network Manager automatically associates that Site ID with inventory entities created within the context of the site. That Site ID then appears in any database filter whenever users retrieve data within the context of a site, ensuring that the results come only from the site in context.

The one exception to this rule of filtering is that, from the MSP's perspective, no Site ID limits the visible data set, regardless of the organizational site. Inventory entities only exist within a single site since they hold a single site ID.

The following entities use this approach:

- Resources
- Services
- Policies
- Authentication
- Discovery Profiles
- Locations
- Contacts
- Alarms
- Events
- Event Processing Rules
- Resource Groups
- Audit History
- Schedules
- Performance Dashboards

13

Troubleshooting Your Application

The following describes troubleshooting steps from installation to execution of this application. Installation logs are in the directory `$OWARE_INSTALL_ROOT`. Log files are `setup.log`, `app_setup.log`, and `db_setup.log` (this last log does not appear if you install an Oracle database).

NOTE:

Because this software installs in many different settings, and permits many add-ons and options, not all troubleshooting tips may apply to your installation.

Troubleshooting Prerequisites

Before you begin troubleshooting any serious problem you will need the following:

System details

- Hardware specifics (as applicable)… processor, memory and disk (free space, and so on).
- Operating system and version?
- OpenManage Network Manager version
- Browser and version? Java? Flash?
- Single or distributed installation? Clustered?

Environment details

- How many managed devices?
- Main features used?

Troubleshooting

- Screenshots of errors
- Logs (the `logs.jar` file produced by running `getlogs`)
- A complete description of the problem, and the steps to reproduce, and a complete description of anything already tried that did not work.

Mini Troubleshooting

Suggested mini-troubleshooting steps for a balky application that is already installed and running:

1. Refresh the browser. If that does not work...
2. Clear the browser's cache (Firefox in particular loves persistent old pages), then refresh.

When you see a difference between direct access behavior between browsers on two different machines, delete temporary internet files. In Windows, open control panel, and open Java. Click the *Settings* button in the *General* panel, and click *Delete Files*. Delete for *Applications and Applets* and *Trace and log files*.

If that does not work...

3 Stop and start the browser. If that does not work...

4 Stop and start the web server

For Windows, to start the web server manager: `oware\synergy\tomcat-X.X.X\bin\startsynergy`. For Linux.

`/etc/init.d/synergy start` or `/etc/init.d/synergy stop`
Worth noting: The tray icon for the web server () is "optimistic" about both when the web server has completely started and completely stopped. You cannot re-start web server when its Tomcat process still lingers. If you lack patience, kill the (large) Tomcat process then re-start web server. The smaller one is that tray icon.

If that does not work...

5 Stop and start application server. Command lines for this:

`stopappserver` and `startappserver`

If that does not work...

6 Delete the contents of the `oware/temp` directory and restart application server. If that does not work...

7 Reboot the host and re-start the application server, web server and browser.

When troubleshooting (or contacting technical support), you may find pertinent information in logs located in the following directories:

```
..\oware\jboss-5.1\server\oware\log
..\oware\temp\soniqmq.log
..\app_setup.log
..\db_setup.log
```

You can also run `getlogs` from a command line.

NOTE:

If you see errors that say your Linux system has too few threads, make sure you have set the file handles correctly.

Troubleshooting Adobe Flash

Installing the latest Flash version is a part of OpenManage Network Manager's requested prerequisites. When Flash is not installed on the browser, things like Visualize My Network, selecting a license file, importing a file, selecting an OS image to import, and so on, do not work. Selection dialogs require installed Flash to select files from the local system. When Flash is not installed, such buttons appear to be active but they do not work.

covered in Revising Database Aging Policies

~~Database Aging Policies (DAP)~~

~~DAP policies automatically purge or archive stale data so the database can maintain its capacity. Several pre-defined and pre-seeded DAPs come with OpenManage Network Manager. You may need to revise these to fit your system. These start at specific times—see the Schedules portlet for specifics about when.~~

~~DAPs amount to preventative maintenance since they help to maintain the database's capacity. Best practice is to do the following regularly:~~

1. ~~In the Audit Trail Manager, create a Filter for Creation Date = prior Month and Action = DAP Executed.~~
2. ~~Review the records for Status – Failed. These indicate that a DAP job failed. As long as the following DAP jobs execute, no immediate action is required. If any DAPs are repeatedly failing, then consult the troubleshooting document or OpenManage Network Manager support.~~
3. ~~Review the DAP jobs entries and compare to the scheduled DAP start times. Confirm that audit records are displaying a corresponding audit record for each scheduled execution.~~

Installation Issues

If you are having difficulty installing the application, refer to the *OpenManage Network Manager Installation Guide*, Preparing for Installation section may help you resolve installation problems.

Installation File Issues

When installing from a compressed file, file corruption can result from an incomplete file copy, or (FTP) transmission. One symptom of corruption: the file will not unzip. Corruption can also appear when you copy unzipped installation files from Windows to Linux. These can pick up erroneous line feed characters. **Workarounds**:

- FTP installation files from Windows to Linux
- Copy the entire ZIP or compressed file first, then uncompress/unzip it.

Installer Failure

- The installer fails, and you are installing on Windows 2012 (this error appears: `Installer User Interface Mode Not Supported.`
  Workaround: Right-click the `win_install.exe` file, and, in *Properties*, select compatibility mode for Windows 7 or Vista before (re)initiating installation.
- If you created an installation CD from unzipped package:
  -CD formatting limitations can truncate file names to eight characters
  `-Setup.log` complains about the absence of the `owareapps` directory
  -The directory name is truncated to `owareapp` (no "s"), `win_install.exe` becomes `win_inst.exe`

  Workaround: FTP the zipped package. If you are burning an installation CD, use the ISO file, and something like the `mkisofs` utility as the input to the CD-ROM burner.

Additional Windows problems include the following:

- Installer does not provide options to select the desired network interface card / IP address.

Workaround: Remove the line `InstallMode=Simple` from the `setup.ini` file in the installation source directory. This enables installation in `standard` mode which provides installation options and detection of a second network interface card (NIC).

- Installer fails immediately with error `Create Process failed ==> %1 is not a valid Win64 application.`
  Solution: Change the value of the `%TEMP%` environment variable. Change the default value of the `%TEMP%` environment variable to another path you have already configured, for example: `C:\Temp`. Use the Windows System Tools menu to do this.
- The installing user must have write access on target directories where the application is installed.
- The same user who installed the software must initiate any uninstallation. Uninstalling may also encounter locked files and directories. This may leave files and directories behind since locking prevents their deletion. For completeness' sake, recommended practices are manual deletion or the use of an unlocker program. Clean directories are important, particularly if you are uninstalling then re-installing,

Other Installation Issues

You may see messages like `failed to reset password`. The following deals with this and other potential problems:

- Make sure you can resolve the hostname to the correct IP address:
  `ping -a [IP address]` and `ping [hostname]` and make sure they are in sync.

  If the application becomes unusable after changing the application server IP address (post-install).

  Solution: To change the application server IP address:

  1. Shutdown application/web server
  2. Open command prompt/shell and source environment. (for Windows: Type `oware`, for Linux: Type `.[space]/etc/.dsienv`, meaning: `. /etc/.dsienv`)
  3. Modify `oware.appserver.ip` property in file `[installation root]\oware\synergytomcat-x.x.x/webapps/ROOT/WEB-INF/classes/portal-ext.properties`.
  4. Verify the file does not specify the old IP anywhere else. If it does, replace with new IP address and save.
  5. Next, modify the IP address in any shortcut URL properties and click OK. `[installation root]\oware\synergy\tomcat-x.x.xx\bin\portal.url` (Web Document tab)
  6. Type `ipaddresschange -n <new IP address>` in a command prompt/shell.
  7. Restart application and web server.
- Ensure any other of the application's installation(s) have been completely removed, if you have uninstalled a previous version.
- Make sure no other MySQL databases are installed (some Linux packages include them by default).
- You must be user with administrator permissions to install.

Standalone Database Installation Problems

- Errors appear after installing a standalone database, even though its connection has been verified successful using pingdb utility.

  Solution: After setting the environment in a shell (Windows: `oware`, Linux: `. /etc/.dsienv`) Verify the following commands have been run on the application server.

  - `loaddb` (create OpenManage Network Manager database)
  - `loaddb -d` instead of `loaddb` if the tablespace has not been created.
  - `loaddb -s` (create synergy/portal database)
  - `oraclepostinstall` (seed components and resolve database schema changes)

  After confirming the above, start the application server and synergy portal after application server is up/ready.

Install-From Directory

Installation package files must not be in the installation destination directory.

Installer Logs

Installation logs are in `$OWARE_INSTALL_ROOT`. Log files are `setup.log, app_setup.log,` and `db_setup.log` (this last log does not appear if you install an Oracle database). An empty or missing `app_setup.log` means no applications were installed. This can result from a truncated `owareapps` directory name. **Solution:** Correct the directory name and attempt the installation again.

Startup Issues

The following are some possible problems with application startup. Remember: after you first install this application, the application server takes longer to start. Be patient the first time you start the application.

The two most common reasons for the inability to start an application server which worked previously are the following:

Application Server Does Not Start

To find application server issues, search the server log (`\oware\jboss-x.x\server\oware\log\server.log`) file for the word `error`. Review the log for the first error or exception. This is typically the item that needs to be resolved and the most relevant for troubleshooting information.

- Installation checks to confirm your hardware is adequate, but if you are installing to a VM, you can reduce hardware allocations after that installation. If you do that, your application server may not start and will provide no logs. This indicates you may have inadequate hardware or an inadequate portion of your hardware assigned to the VM running OpenManage Network Manager. If this occurs, check the hardware requirements, and reconfigure your VM, or install on a different machine.

  - Check the total system RAM

  - Check the appserver heap setting in `/owareapps/installprops/lib/installed.properties`. If it exceeds the total system RAM either you must allocate more RAM or reduce the appserver setting

Application server should never be allocated less than 3G ram, and Web server should never be allocated less than1G RAM.

- The following socket errors (or similar) are reported when starting the application.

```
(Feb 14, 2014 4:57:50 PM) [OWProcessMonitor] ERROR! command socket
   failure: Address already in use: Cannot bind
(Feb 14, 2014 4:57:50 PM) [OWProcessMonitor] re-initializing command
   socket: attempt 1 of 10
```

  This indicates a port conflict is likely preventing your system from functioning properly. This typically occurs when network management or other applications reside on the same server. Determine the source of the port conflict and remove the application. Best practice is to install on a dedicated server platform.

- Port Conflicts, as described in the previous paragraph, can arise after installation. For example if you install other software that uses the SNMP ports (161 and 162), after you have installed OpenManage Network Manager, the installation cannot catch such a conflict. When you try to start it, application server will report it cannot bind to that port, and fail. See Ports Used on page 697 for a list of potential conflicts. The `server.log` file lists to such errors when they occur.
- Confirm your license is current and installed. Search the `\oware\jboss-5.1\server\oware\log\server.log` file for `error`, and the license expired error appears.

  To install a license file without a running application server, run the `licenseimporter` script:

  ```
  licenseimporter license.xml
  ```

  Your license may have a different name, but the script syntax is the same.

Permission issues caused by license

You receive the "You do not have a permission to view this application" message, it most likely means that you have an expired feature license.

Solution:

For Virtual Appliance:

1. Re-apply vmlicense.xml located in the /home/synergy directory
2. Apply the Dell EMC generated SKU license if you received one.

For Non Virtual Appliance:

1. Re-apply the license.xml file located in the ..\OpenManage\Network Manager directory
2. Apply the Dell EMC generated SKU license if you received one.

No valid HA license is found during installation of HA

After installation of the secondary appserver, the primary server goes down (appserver icon changes from green to red), this most likely happened because incorrect license was applied for HA package. To check the status why appserver went down, right click on the appserver red icon and select logs/server option and search for Beginning Server Shutdown. You will see:

2015-08-05 13:02:59,738 3040923 FATAL [com.dorado.mbeans.OWClusterPeerActiveImpl] (Timer-8:) APPLICATION SERVER ERROR

2015-08-05 13:02:59,739 3040924 FATAL [com.dorado.mbeans.OWClusterPeerActiveImpl] (Timer-8:) License Not Found for Clustering Servers in High-Availibility Mode

To resolve this issue, contact Dell EMC Support to generate an HA license. Once HA license is received, place it anywhere where appserver is installed then bring up web client and log into OMNM. When at home page, select "License Management" and click on "Select File" button. Navigate to where the license file is located and click on "Open" button. At this stage, after few seconds, you should receive a popup message stating that license got imported. Restart appserver.

Startup issues for Windows installations

If an application or mediation server goes down ungracefully for any reason the JMS message database may be corrupt in `$OWARE_USER_ROOT\oware\jboss*\ server\oware\data`. When it becomes corrupted the application or mediation server cannot start.

Workaround: Delete the content of the `data` directory. This allows application or mediation server startup.

See Linux Issues on page 404 for additional information about troubleshooting Linux.

Initial Logon after installation fails

If, after installation, your attempt to logon to the application fails with message `Connection to server failed` in the Logon window.

Solution: The most likely cause is that the application server is not running. (Re)start it.

The icon in the Windows System Tray or the presence of the `java.exe` process indicates the status of the application server.

If the icon is red or yellow, no client can connect (although some portlets appear without the benefit of application server). If the icon is red, right-click on it and select *Start* from the menu. The icon turns yellow as the application server starts. Wait until the icon is green, and repeat the logon procedure. If this does not work, contact technical support.

Direct Access Fails Because of Java Security Settings

Some Java installations' security settings (in v.1.7+) may block self-signed websites, interfering with Direct Access. The workaround is to provide a security exception for the application server, as follows:

1. Click Start
2. Type configure java and hit [Enter]
3. Select the Security tab.
4. Click Edit Site List
5. Click Add
6. Type the OpenManage Network Manager URL (example: `http://192.168.0.51:8080/`. Best practice is to use the IP address of the application server, not `localhost` or `127.0.0.1`)
7. Click OK and Continue.
8. Apply this change, and/or click OK.

Logon Fails with Invalid Logon Message

When you enter your User Id and Password in logon dialog and click Logon, an Invalid Logon message appears.

Solution: Ensure you are entering the correct User Id and Password and click Logon. If you have forgotten the User Id or the Password, or if another user has changed the Password for the User Id, you may have to re-install the software.

Mediation Server on separate machine fails

Distributed mediation server failures to start can occur when multicast is disabled on your network. The workaround is to this property in
`owareapps\installprops\lib\installed.properties`

```
oware.application.servers= [application server IP address]
```

Correct this on all mediation server machines.

Unsynchronized Clocks in Clustered Installations

All machines in a cluster, or distributed system, must have synchronized system clocks. If this is not true, systems may start, but will not work correctly.

Other Failures on Startup

- Another instance of appserver/medserver may be running on one host. Common error contents:

```
2005-06-25 08:47:51,968 ERROR [org.jboss.web.WebService] Starting failed
java.net.BindException: Address already in use: JVM_Bind
at java.net.PlainSocketImpl.socketBind(Native Method)
```

Solution: Stop and if necessary restart application server(s).

Starting and Stopping Servers

Best practice in Windows installations is to start or stop application server with the process monitor icon (installed by the application), when it is installed as a service. Stopping, starting or restarting the service through operating system's Service Manager is not recommended. If the status icon in the tray is green and you restart procman ("process manager") from Windows' Control Panel services, an error message appears saying the service did not stop properly. The tray icon then turns white. Since the application server is still running, when you try to restart the service again, the icon turns red.

To restore the Process monitor icon to function correctly and show status, stop all Java and WMI processes in the process manager. A system reboot also re-initializes the OWProcMan (process monitor). Note that the service name may be different if your package has been specifically branded. The executable path for the service is `\....\oware\bin\owprocman.exe`.

More Failures on Startup

- Failure to connect with a database can occur when...
  - –The Oracle instance not running
  - –Oracle or separate MySQL lacks connectivity. Use `pingdb -u <user> -p <password>` to check. Default user/password for MySQL: root/dorado
  - –Oracle database is not built, or you have not completed its installation
  - –MySQL not running (it should start automatically)
  - –Your firewall blocks ports the database needs.
  - –You see `ERROR..java.lang.OutOfMemoryError` in the log file.

The following will solve failure to see a login screen in web client:

1. Shutdown web server
2. In a command shell type the following: `oware`
3. Type `mysql -u root --password=dorado` This will log you into mysql database

4. Copy and paste into mysql shell and hit enter:

update lportal.layout set typeSettings = `'layout-template-id=1_column\ncolumn-1=58,\n'`

where (`groupId=10180`)

AND(`privateLayout=0`)

AND(`friendlyURL='/login'`);

5. Restart web service.

6. Log into OMNM > login form comes up

- Changed properties files
  –Delete the contents of `oware\temp`
- Connection to application server fails
  –Application server has not fully started. Look for `>>>>> Oware Application Server initialization COMPLETE. <<<<<` in the `server.log`

Login Failures

- Invalid Logon
  –Incorrect log in ID or password (the default for web client is User *admin*, password *admin*)
  –User has changed and forgotten password
- Account is inactive
  –Application Security Policy may be configured so passwords or accounts have an expiration date.
  –Use different account.
- Memory errors that indicate too little memory on the application server can also prevent login.

Multi-NIC Host Fails to return to the portal—When you click the *Return to ...* link from Control panel, some unexpected URL appears in the browser. To see the root of this problem, go to *Portal* > *Portal Settings* and compare the *Virtual Host* entry to the application server's IP address. If they are different, then DNS has two different IP addresses associated with the same hostname. OpenManage Network Manager needs an unambiguous IP address and associated hostname for both application server and client.

Workaround(s): 1. Use a local host file and map the IP selected during installation to the hostname. 2. Set the DNS server to only resolve the selected IP address to this machine's hostname.

- Installer fails immediately with error `Create Process failed ==> %1 is not a valid Win64 application.`
  Solution: Change the value of the `%TEMP%` environment variable. Change the default value of the `%TEMP%` environment variable to another path you have already configured, for example: `C:\Temp`. Use the Windows System Tools menu to do this.

Troubleshooting Flow

As part of the troubleshooting process, you can often determine the culprit for problems by a process of elimination. The following questions may help determine what is the real issue:

Discovery / Resync

See Communication Problems on page 383, Preventing Discovery Problems on page 383 and Discovery Issues on page 384

- Can you ping the device you are having difficulty discovering? If you can ping them, and have discovered them, but ping still does not work from within the application, do the devices have an ICMP management interface when you right-click > *Edit* them? If not, add the interface and resync.
- Is your system permitted access to the device (on the Access Control List)?
- Are firewalls blocking access to the device(s)?

NOTICE

The command `service iptables stop` turns off the Linux firewall. Turning it off temporarily is recommended when you first install.

- Is any other software on the application server / mediation server host causing a port conflict? (Uninstall it)
- Is SNMP is configured on the target device and read/trap, write community strings? Is SNMP correctly set up? (check with Network Tools and MIB browser or a tool like iReasoning's MIB browser)
- Is Telnet or SSH configured on the target device and can you Telnet / SSH to the device through a command line shell or an application like puTTY?

NOTE:

Some devices support only SSH v2. Consult release notes for specifics.

- Are authentications created in the Authentication portlet with protocols and passwords set correctly, with adequate timeout and retries configured for your network's latency?
- Are Discovery Profiles using the created authentications?
- Does device fail to resync after deployment?

  wait up to a minute before resync as SNMP agent is not enabled yet on the device.

Backup / Restore / Deploy

See Backup / Restore / Deploy on page 385

- Is your FTP server installed, up and running?
- Is that FTP server on the same side of the firewall as the devices it addresses?
- Does the device support the type of backup (FTP, SFTP, TFTP) you are attempting?
- Do your authentications grant privileged access? The prompt is typically #, not > at this level of access.
- If the device does not successfully execute the command, then either the authentication you have used does not have permission to do such commands, or the device is configured to prohibit their execution.
- Do FTP and TFTP servers write to the same directory, and have permissions to read/write/execute to that directory?

Alarms / Monitors / Performance

Consult the User Guide's recommendations, particularly for Monitoring and for Traffic Flow Analysis. See Alarm / Performance / Retention on page 386.

- Do you have the recommended hardware to handle the number of devices you are managing?

- Are the devices you are monitoring sending only the relevant traps to your system?
- Is your database configured correctly for the expected load? Symptoms of database configuration inadequacies include slow performance when expanding the Resources portlet or right clicking on a port of a device and selecting show performance. This can also occur if your database size has increased significantly since implementation.

  Solution: For MySQL, adjust/increase the innodb_buffer_pool_size to restore performance. Consult the User Guide for more about performance tuning such parameters in MySQL.

  NOTICE

  The internal event `emsDBCapacity` notifies you about how much of the database you have used.
- Have you tailored your monitoring to the available capacity of your hardware? Monitoring or other functionality dependant on writing to the database may stop with error specifying

  ```
  Could not get a database connection
  ```

  One example of an error that appears when an active monitor which is suddenly unable to insert data into the database

  ```
  2014-04-10 11:14:47,376 490736076 ERROR
      [com.dorado.broadscope.polling.PollingResultsDAOImpl]
      (WorkerThread#8[71.192.23.246:58220]:) persistsPollingResults failed.
      Rolling back.
  com.rendion.ajl.CheckedExceptionWrapper: Could not get a database
      connection.
  ```

  Solution: If the database can be reached over the network and has been confirmed operational/healthy, the configured pool allocation(s) may be exhausted. Refer to the *Installation Guide* and confirm sufficient pool allocations have been configured for corepool, jobpool, and userpool.

  The *Installation Guide*'s Clustering chapter contains suggestions for properly sizing pool values based on the number of servers in your environment. Based on this information and your current configuration, increase pool values accordingly.
- To isolate the source of performance difficulties, does un-registering Traffic Flow exporters, or turning off monitors have an impact?
- Not receiving flows in Traffic Flow Analyzer? Make sure that router/switch is configured to send sFlows using port 6343 and NetFlow/jFlows using port 9996.

Hardware

See Environment / Operating System Issues on page 415.

- Does your hardware match the system recommendations for the number of devices managed, monitoring and concurrent users?
- Have you followed the installation recommendations (particularly important for Linux) in this guide and *Installation Guide*?

Advanced Troubleshooting

If you remain unable to resolve issues with your system, the following may be helpful.

- When you contact technical support, create a `logs.jar` file with the `getlogs` command, so you can forward it to them.
- You can change the messages your system generates. That may be necessary. See Debug on page 392.

This chapter contains more troubleshooting advice like WMI Troubleshooting Procedures on page 395, and Linux syslog not displaying on page 406 (setting up devices for various vendors).

Upgrade / Data Migration Fails

I. Unexpected Database Behavior after Upgrade: If you observe unexpected behavior after an application upgrade, review installation logs. Confirm evidence appears that the upgrade executed `dbevolve`. If not...

Solution: Execute the following steps

1. Shut down the application.
2. Open a shell/command prompt on (the primary) application server.
3. Execute command `oraclepostinstall`.

   This step resolves potential database changes between application versions. You must run the command for both MySql and Oracle database environments too.

II. Upgrade Fails with Database Connection Failure: If an upgrade installation fails with the message with the `app_setup.log` error `Connecting to database...>>>>> ERROR: OWSessionIDRDBMS : Failed to make database connection`, the problem is that the database is not running on the host being upgraded. To cure this problem, manually start the database, and then re-try the upgrade installation. The following are the startup commands for the embedded database:

Windows:

```
net start mysql
```

You should see the following response in the shell where you execute this command:

```
The MySQL service was started successfully.
```

NOTICE

If you substitute the word `stop` for `start` in the above, these commands manually stop the database.

Versions

Before you begin more in-depth troubleshooting, you may need to know what versions of various components are installed to ensure they are compatible. To see these before installing, consult the `version.txt` file in the installation source's root directory, or after the application is running, view its *Manage* > *Show Versions* screen. Differences between `version.txt` and *Show Versions* may occur when you install additional applications or patches.

Another way to see the versions for currently installed modules: open a shell (*Start* > *Run* `cmd` in Windows, for example), and type `oware` (`. /etc/.dsienv` in Linux) and [Enter]. Then type `showversions`. The currently installed modules and their versions appear in the shell. You can also use the *Manage* > *Show Versions* menu in web client to find this information.

Search Indexes

Sometimes this software may display Control Panel objects like Users, Roles, and Organizations inaccurately. This occurs because Search Indexes need to be re-indexed every so often, especially when changes to Roles, Users and Organizations are frequent.

To re-index go to Control Panel > Server Administration and then click on the *Reindex all search indexes*. Reindexing is not instantaneous; expect this to take some time.

Communication Problems

Firewalls may interfere with necessary communication between elements within or monitored by your system. Best practice when installing is to bring the firewall down, install, then once you have confirmed the installation runs, bring the firewall up with the appropriate ports open. (See Resolving Port Conflicts on page 393, also see Ports Used on page 697 and Ports and Application To Exclude from Firewall on page 708.)Managed devices often have Access Control Lists (ACLs) for management traffic. Best practice is to use a management VLAN or subnet. Note also that in-path devices may filter management traffic creating an obstacle to management messages. Overlapping address spaces may also complicate network management. Identifying such "DMZs" and overlaps is part of network analysis.

Preventing Discovery Problems

Ensure your firewall is not blocking network access to equipment you are trying to discover. The following describes more preventive practices to do when you discover a mixed vendor / mixed class network.

ICMP (Ping)

You can ping devices from a shell or the Network Tools portlet to insure it's up and online.

Telnet / SSH

1 Manually telnet or SSH connect to a device to verify that you have the correct authentication information (although Discovery Profiles' *Inspect* function does this too).

> **NOTICE**
>
> Later versions of Windows do not include telnet by default. In addition to free telnet programs you can download and install, like PuTTY, you can open a shell (*Start* > *Run* `cmd`) and type `oware` to get telnet capabilities. **Also:** Use SSH v2 for Dell devices.

2 If you know the device, look at its configuration file and verify that the SNMP community string is correct.

3 Discover the device.

4 If there are any problems with any devices, then ping them, and/or telnet to problem devices and verify that telnet works / authentication is good.

5 If SNMP problems arise, use this application's MIB browser tool to troubleshoot them.

To verify SNMP and WMI connections are working between your system and the devices in the network, use the following tools:

SNMP

1 Open MIB Browser in the web client's Network Tools portlet, or by right-clicking the device.

2 Select RFC1213, system, from the RFC Standard Mibs branch

3 If necessary, fill out the Authentication tab

4 Select the device tab and information will populate as soon as the query is answered.

WMI

If you are discovering WMI systems on your network, the following may be helpful.

1 Launch the `wmiutil.exe` command line tool from `\owareapps\wmi\bin\"`

2 You need to supply a user and a password along with an IP or hostname

Typing `wmiutil.exe` with no arguments returns launch the WMIUtil User Interface.

```
c:\Dorado\owareapps\wmi\bin\wmiutil.exe -user <user> -password <password>
   -host <IP or Hostname>
```

Typing `wmiutil.exe ?` at a command line returns what parameters are available for the command line version.

NOTE:

Even if you do not need a domain to log into your WMI device, the graphic interface for this utility does not work if the domain field is blank. Any content makes it work correctly.

See WMI Troubleshooting Procedures on page 395 and Additional WMI Troubleshooting on page 402 for additional details.

Discovery Issues

Discovery may fail if its authentication or network parameters do not match the configuration of devices discovered. Here, the results panel typically displays a message like `No Devices were detected with selected Discovery Parameters`. Use the *Inspect* function in Discovery Profiles to validate credentials entered.

Some additional sources of Discovery issues, and their solutions:

- Equipment with management IP Addresses in the selected subnet, range, and so on does not exist. Correct the selected range and retry.
- The equipment in the selected range has already been discovered.

  Managed devices can only be discovered once. Those devices that have already been discovered appear in the Discovery Results section of the Discovery Wizard. Update the state of previously discovered devices by selecting *Resync* from the right-click menu. If you want to re-discover these devices, delete them from the Managed Resources portlet
- The SNMP community strings / authentication on the equipment do not match the default values used by this application. Correct the SNMP authentication selected for discovery.
- Discovery finds a device, but features like Direct Access, Backup and Actions do not work.

  Solution: The device likely has a correct SNMP authentication, but an incorrect CLI (Telnet / SSH) authentication. Either re-run the Discovery Profile after deleting the device and correcting the authentications, or right-click to edit the device and add the CLI authentication and management interface, then right-click to resync the device.

  Note that you must log into the device as a user with enough permissions to accomplish all discovery and other tasks. If you log in as a user with limited permissions, then discovery results reflect those limits.

  NOTICE

  The *Inspect* feature of the Discovery wizard lets you validate authentications.

  Alternative: The device is not supported by your current license or driver set. To request support, use the MIB browser to navigate to RCC1213 ifTable details, and export / save this branch. Navigate to ENTITY-MIB entPhysicalTable details and export / save this branch. Attach the exported files to e-mail to support, or to a trouble ticket.

The following describe additional discovery issues.

HTTP Authentication

Often, an HTTP session with devices that support it exchanges data with the device after discovery. This process fails if the HTTP Authentication information is incorrect. Create HTTP authentications that match your devices' in the Authentications portlet and use it in discovery.

Device O/S Overrides

The device driver installed must support the Operation System version on that device. Verify the equipment's firmware and operating systems are among those supported. Supported firmware and operating systems appear listed in the release notes, or in *Manage* > *Show Versions*.

Example: Override driver-unsupported operating systems for the Juniper devices in `/owareapps/juniper/lib/juniper.properties.` Change `com.dorado.juniper.supported.OS.dc.default.max`

This revision does not support new features. Other device drivers have similar override mechanisms.

If devices appear in Managed Resources as Discovered Entities, rather than specific vendors' devices. This can mean the following:

- The equipment's driver is not installed.
- The driver installed but not seeded to database. `Workaround:` Run `ocpinstall -s` on a command line.
- Monitored devices must be configured to connect and send SNMP traps to the element management system.

If your system discovers only top level equipment, this can mean the following:

- Devices do not have components (interfaces, ports, and so on).
- An incorrect telnet / SSH authentication can have an incorrect password or no enable password. **Workaround:** You can right-click and edit the equipment with this problem to add the telnet / SSH authentication. Make sure you also add a management interface, then resync the device.

Backup / Restore / Deploy

Failures of backup/restore capabilities often stem from failures in the external FTP/TFTP server. This means the FTP / TFTP server is offline, blocked by a firewall or incorrectly configured. Check in the File Server Manager to correct this. Also, on such servers, FTP and TFTP server must share a directory, and the directory must have all permissions to permit these servers to write, read and delete temporary files.

If deploying firmware fails with the following symptoms:

- Selecting *Deploy* does nothing.
- The FTP/TFTP File Server status is Disabled.

  Workaround: Back up the device first to validate it is connected with the FTP server.

When you use the file backup (NetConfig) option, the internal FTP/TFTP server is provided for testing, not production; do not use it. External FTP servers are essential for performance reasons, and, if necessary, the network equipment using FTP to send/receive configuration files must have FTP enabled.



NOTE:

If you have separate FTP and TFTP servers, they must read/write to the same directory.

If deploying firmware succeeds, but device doesn't reboot:

That might be because of "Console Logging" is enabled. Please disable console logging. The messages from console logging interfere with the communication between OMNM and the device (via CLI) and can disrupt supported functionality in OMNM.

Timeout

Timeout can occur when backing up / restoring large config files.

Workaround: Change timeout values in the telnet/SSH authentication object. Right-click > Edit the device and change those values in the Authentication tab. Typically this means doubling the timeout, and increasing retries to 2 - 3 times.

NOTE:

Secure FTP connections (scp/sftp) often require SSH services be enabled on the devices addressed. Ensure your system's server and sftp/scp file server can access the devices with SSH too.

Group File Management Failure

If group file management backup operations fail for some devices while individual backups to these devices are successful, typically thread pool-related backup errors appear in logs during the related time frame.

Solution: Your system may have insufficient threads available to handle the number of concurrent tasks required by the group backup operation. Some threads could have already been in use for other tasks when the group operation began.

To address this, increase the size of the thread pool to handle additional concurrent tasks with the following steps:

1. Shutdown application.
2. Edit `owareapps/installprops/lib/installed.properties`
3. Add the following property...

   `ProvisionThreadPoolMBean.PoolSize=70`
   (Adjust as needed based on current setting and need.)
4. Save `installed.properties`.
5. Start application.
6. Execute the group backup operation.

By increasing the Pool Size, the application can perform additional concurrent tasks that fall within the scope of this pool.

Alarm / Performance / Retention

If you install your system to monitor alarms, and experience sluggish performance or a rapidly filling database, several remedies are available.

- Configure "chatty" devices emitting many alarms to stop doing so.
- Configure your system's Suppress Alarms feature to keep performance the database's capacity at acceptable levels
- Reconfigure your system's database archiving policy feature to archive alarms more often so the database does not fill up.

Retention Policies

Retention policies tune how long your system retains data. These policies also have built-in limits (raw, hourly, daily) that help to avoid potential performance/storage problems. The potential impact when going outside these thresholds is significant and generally not recommended.

Configure retention policies with the following limits in mind:

- Maximum # of days to retain daily data: 180
- Maximum # of days to retain hourly data: 14
- Maximum # of days to retain raw data: 1

Network Monitoring

You can monitor your network's performance two ways.

- Scheduled polling-based monitoring is more reliable, and specific. It also has a lower impact on network. It may, however, lag behind network events.
- Event-based monitoring (typically Traffic Flow Analysis, syslog and SNMP) is more up-to-date, but, can be less reliable. It also often does not disclose the root cause of a problem.
- This software does not support Traffic flow analysis on sFlows from devices using sFlow earlier than v5. Typical error content reads "Data array too short" if you have an unsupported sFlow version.
- Traffic Flow Analyzer support in OpenManage Network Manager collects and process flows with source and destination IP address. Switches or devices that only support L2 flow payloads with MAC address as the source and destination payload are not currently supported. Example: Juniper XE devices.

NOTE:

Typical packages come with a default limit to the number of monitored devices. Upgrade your license if you want to exceed the package limit. Because of the performance demands they make, Traffic Flow exporters are licensed separately from the managed resource license count, so a license to manage 50 devices does not necessarily let you have 50 Traffic flow exporters.

Also: The application discards IP v6 flow packets.

NOTICE

Does Traffic flow not appear when it's expected? Have you made sure the device is registered to display traffic flow (right-click in resources *Traffic Flow Analyzer > Register*)?

- Each monitor should have 10,000 or fewer targets. Use a new monitor to track any targets exceeding that number. The general best practice is to have fewer targets distributed across several monitors.

Using this software's features, you can create alarms and reports for each. Best practice is to use both polling and event-based protocols. Tune the polling frequency and event granularity for the specific environment, topology, bandwidth, and notification needs. See the specific Monitor performance recommendations.

NOTICE

Creating a baseline performance measurement report of availability, capacity and performance can provide the basis of capacity planning and proactive network management.

Reachability may vary by protocol (for example, Telnet works, but not ping), so test multiple protocols. If it is remote, try phoning the affected site and asking for information.

Missing Performance Data / Monitor Stops Polling

This is a problem related to missing performance monitor data accompanied by logs errors like the following:

```
2014-02-12 11:23:45,357 705304239 ERROR
    [com.dorado.core.mediation.base.OWMediationDeploymentHelper]
    (WorkManager(2)-63:) The currently deployed targets for polling
    subscription oware.polling.PollingSubscriptionDO::59x8vSybkeEj6I2 on
    mediation partition MED_PART-medPartition have somehow become out of
    synch with the application server and database.
Actual target count, coming from the database: 184 meditation server
    currently has: 0
We are now resynching this information from the appliation server to the
    mediation server so that it will once again be accurate.
```

This error indicates that your mediation servers have no current performance monitor subscription targets when 184 targets were expected. This could possibly be due to a mediation server fail-over to another cluster member or a mediation server coming back on-line, etc. This is an expected error when a difference is detected in the expected (database) monitor subscriptions and actual subscriptions in the mediation server. A periodic process executes to ensure performance monitor subscriptions remain in sync.

Solution(s):

- Verify connectivity between application servers and mediation servers.
- Verify mediation server state/health and cluster member status (active/inactive).
- Verify polling subscriptions in the Monitor Editor.
- Verify polling skip/miss counts in the Monitor Editor.
- Review number of targets in each monitor, verify each has 10,000 or fewer targets. Monitor any targets over that figure in a new monitor.
- Restart the mediation server process if subscription problems persist.

Reports

- I created a report and didn't specify a location. Where's my report?
  Solution: The default location for reports is `/oware/temp/reportfw` under the installation root.

Report Missing Data

This software limits reports to 5000 rows by default when saving reports to the database (*Save* checkbox checked). This limit does not apply when not saving and only exporting the report. Increasing this default value is not best practice because of potential performance impact.

Solution: If you must increase the size of reports you save, increase the following report-related property values and restart application server(s).

```
com.dorado.redcell.reports.max.report.size (Increase to save larger
    datasets to database - not recommended)
com.dorado.redcell.reports.max.report.query.size (Increase to include more
    data in exported reports)
```

Follow these steps:

1 Edit `[Installation root]owareapps/installprops/lib/installed.properties` and add/modify the desired properties.

```
com.dorado.redcell.reports.max.report.size=<new value>
com.dorado.redcell.reports.max.report.query.size=<new value>
```

2 Restart application server(s).

Web Portal

Web portal problems can occur as described in the following section:

I. Web portal performance is slow or login page inaccessible.

Solution: Check/verify portal memory heap settings and increase as needed.

To manually change the web portal heap settings, verify sufficient system memory exists then modify the setenv.sh (Linux) or setenv.bat (Windows) file:

```
set "PORTAL_PERMGEN=768m"
set "PORTAL_MAX_MEM=4096m"
set "PORTAL_INIT_MEM=4096m"
set "PORTAL_32BIT_MAX_MEM=768m"
```

These files are in the `[Installation root]\oware\synergy\tomcat-x.x.xx\bin directory.`

For Linux, restart the portal service to apply new memory settings. In Windows, besides updating `setenv.bat` you must run `service.bat update` in that same directory.

II. Web Portal Displaying Errors: The application web portal displays errors immediately after starting application processes.

Solution: Allow the application/web server more time to fully start before attempting to access the web portal.

III. Web Portal Down, Cannot Access/Display Login Page: The application web portal displays errors or cannot be accessed.

Solution: Verify the Portal Oracle database password has not expired. By default, `netview` is the default user to connect to database. This appears in `/opt/dorado/oware/synergy/tomcat-[version]/webapps/ROOT/WEB-INF/classes/portal-ext.properties`

```
jdbc.default.username=netview
jdbc.default.password=dorado
```

Connect using SQL*Plus to set new password, you can even use the same password you had earlier.

```
$ sqlplus
SQL*Plus: Release 11.2.0.1.0 Production on Mon Dec 13 01:12:07 2010

Copyright (c) 1982, 2009, Oracle. All rights reserved.

Enter user-name: netview
Enter password:
ERROR:
ORA-28001: the password has expired

Changing password for netview
New password:
Retype new password:
Password changed

Connected to:
Oracle Database 11g Release 11.2.0.1.0 - 64bit Production
```

After resetting the password, best practice is to set profile/policy expiration to LIFETIME to prevent this from expiring again.

NOTE:

Users `netview` and `synadmin` need to have same password.

MySQL Database Issues

See Optimizing Your System on page 71 for preventive `my.cnf` performance tuning tips.

I. Slow Performance: If your system's performance slows to the extent application is unusable, and its log contains the error below or similar entries:

```
com.mysql.jdbc.CommunicationsException: Communications link failure due to
    underlying exception:
** BEGIN NESTED EXCEPTION **
java.net.SocketException
MESSAGE: Software caused connection abort: recv failed
STACKTRACE:
java.net.SocketException: Software caused connection abort: recv failed
```

Solution: Follow these steps:

1. Review disk space, verify adequate space is available on partition.
2. Shutdown MySQL database.
3. Edit the `[installation root]\oware3rd\mysql\[version number]\my.cnf` file. Review database size configuration and add another data file to extend size as needed. Save file.

   For example: Change:

   ```
   innodb_data_file_path = /ibdata/ibdata1:1024M:autoextend:max:10500M
   ```

   To:

   ```
   innodb_data_file_path = /ibdata/ibdata1:1024M;/disk2/
       ibdata2:1024M:autoextend
   ```
4. Restart MySQL. You can also refer to the following link additional detail: dev.mysql.com/doc/refman/5.1/en/innodb-data-log-reconfiguration.html

II. Tablespace Full / Application crashes. Log entries indicating tables or tablespace are full. Likely accompanied by application crashes. Examples of log entries (which may reflect any table).

```
The table 'rc_notification_hist' is full
```

or

```
InnoDB: Warning: Cannot create table 'owbusdb/pm_dtl_7879' because
    tablespace full
```

Solution: Follow these steps:

1. Review disk space, verify adequate space is available on partition.
2. Shutdown MySQL database.
3. Open `[Installation root]\oware3rd\mysql\[version]\my.cnf` file. Review database size configuration and add another data file to extend size as needed.

   For example, change

   ```
   innodb_data_file_path = /ibdata/ibdata1:1024M:autoextend:max:10500M
   ```

   To:

```
innodb_data_file_path = /ibdata/ibdata1:1024M;/disk2/
    ibdata2:1024M:autoextend
```

4 Save the file.

5 Restart MySQL. You can also refer to the following link additional detail: dev.mysql.com/doc/refman/5.1/en/innodb-data-log-reconfiguration.html

III. MySQL Connection Exceptions: The following error, or similar errors, appear in log:

```
Caused by: com.mysql.jdbc.CommunicationsException: Communications link
    failure due to underlying exception:
BEGIN NESTED EXCEPTION **
java.net.NoRouteToHostException
MESSAGE: No route to host
STACKTRACE:
java.net.NoRouteToHostException: No route to host at
    java.net.PlainSocketImpl.socketConnect(Native Method)
```

Solution: This indicates a connectivity issue between your application server and the database. Discover the root cause of this communication issue and correct it. Here are some things to try:

- Check with `ps -ef | grep MySQL` in Linux or in Windows' Services utility to make sure your database is running. If not, re-install (or uninstall / reinstall) until this daemon / service starts without problems.
- Execute pingdb to test database connectivity.
- Check network interfaces and connectivity between application server and database.
- Try connecting with MySQL Workbench or other tool.
- Verify database is up and healthy.
- Verify database login/password has not changed or expired (default user/password: root/dorado)

IV "Too Many Connections" Error. Ironically, this error may indicate the `max_connections` parameter in your `my.cnf` files is too *small*. To use more connections, change the setting in the `my.cnf` file. For example, in `\oware3rd\mysql\X_X_X-64\my.cnf`, under the `[mysqld]` section add:

```
max_connections = 500
```

You can login to mysql to check current settings:

```
mysql -u root --password=dorado
mysql> show variables like 'max_connections';
```

To check open connections

```
mysql> SHOW STATUS WHERE `variable_name` = 'Threads_connected';
```

Oracle Database Issues

Best practice for Oracle database users is to have a database administrator configure their Oracle application before installing OpenManage Network Manager to use an Oracle database. This ensures correct configuration, best performance and connection with the database.

If you are installing only a single component, rather that a re-installation with the full installation wizard, installation is a three-step process:

1 Extract (`ocpinstall -x [filename(s)]`)

2 Optionally, update / verify the database schema (on database servers only). (`ocpinstall -l [filename(s)]`)

3 Seed the database (on database servers only). (`ocpinstall -s [filename(s)]`)

NOTE:

When using hostname as oracle connection URL, sometime installer may append colon to the URL after the upgrade. **Workaround**: remove the colon from the URL in the installed.properties and portal-ext.properties.

Refer to the *Installation Guide* for more about Oracle databases.

Debug

When an error appears in logs (see Logs on page 394) it indicates for which Java class you need to increase the level of logging if you want debugging information. You can change logging levels to get additional (debug) information.

NOTICE

Best practice is to now alter *Log Categories* in the Application Server Statistics portlet by clicking that button. This alteration simplifies editing `log4j.xml` files since it provides a graphical interface, and if you have more than one server, it alters the log levels for all servers at once.

Flipdebug

You can easily turn debug on or off with the `flipdebug` script. Run this while the application server is running and remember to wait a few moments for the application server to pick up your changes. Here is the usage (just type the script name to see these options):

```
Usage: flipdebug [-d] [-t] [-r] [-h|-?] [-p] product[,product]

-d Turn on debug for all packages
-t Turn on trace for all packages
-p Turn on trace/debug only for product[,product] (no spaces between
   products)
-r Revert to original log4j settings
-h|-? Display usage
```

The *product* name in -p matches the directory under `owareapps`. The debug and trace write to the log and to stdout.

Fine-Tuning Debug

To fine tune debug further, create a file, whose name ends in `log4j.xml` in the `owareapps\installprops\server\conf` directory with the categories you want changed. If the class does not exist within the `log4j` file, add it and set it to debug. Changes preserved in such a file remain in place until you change them again, and are not overwritten when software upgrades occur.

To increase logging levels to DEBUG, change `WARN` or `INFO` to `DEBUG` in categories like the following:

```
-<category name="com.dorado.redcell">
-    <priority value="WARN"/>
-  </category>
...
-  <category name="redcell">
-    <priority value="WARN"/>
-  </category>
```

```
-  <category name="RedCell">
-    <priority value="INFO"/>
-  </category>
```

To see what categories are available, look in `\oware\jboss-x.x.x\server\oware\conf\log4j.xml`. This file concatenates all logging categories, but is generated, and should *not* be changed.

When application server starts, it detects logging levels in these categories and concatenates them into the server's `log4j.xml` from `*log4j.xml` files in the `server\conf` directories of installed components under `owareapps`.

When it starts, application server processes logging for components in order of their dependency, and overrides any detected settings from a file whose name ends in `log4j.xml` in the `installprops` directory.

This application applies detected changes once a minute. The log4j file scanner can then detect any subsequent changes up to a minute after making them. The `server.log` is not truncated when this occurs.

The following are additional categories that allow logging level changes:

For Mediation Server registration with App Server, add the following category:

```
<category name="com.dorado.mbeans.OWMedServerTrackerMBean">
  <priority value="WARN"/>
</category>
```

For SNMP and Syslog, change INFO to DEBUG in

```
<category name="com.dorado.core.mediation">
  <priority value="INFO"/>
</category>
```

To view debug output:

Server

Debug does not appear in real-time in the application server shell (if you have one). View real-time and historical logs in the `oware\jboss-x.x.x\server\oware\log` directory.

> **NOTICE**
>
> Typing `oware` in a Windows shell lets you use Linux commands like `tail -f server.log`. Tailing it lets you watch the log file as it is generated.

Resolving Port Conflicts

Installation scans for port conflicts, but these may arise after you install too. If your application runs with others, conflicts related to those other applications' ports are possible. For example: the application can have trouble communicating with the built-in TFTP server for backups. Port contention of TFTP on UDP port 69 with other applications can cause this. Try rebooting the system to clear any unused ports and verify that UDP port 69 is not in use before starting the application.

Finding Port Conflicts

You can find ports in use with the following command line:

```
netstat -a -b -o | findstr [port number]
```

Use this command to track down port conflicts if installation reports one. Best practice is to run this software on its own machine to avoid such conflicts. Freeware port conflict finding programs like Active Ports are also available.

Logs

You can execute the `getlogs` script to package relevant logs if you need technical support. Run this script in a command shell where you have sourced the Oware environment (in Windows *Start > Run* `cmd,` then run `oware`, or in Linux `. /etc/.dsienv`, and then invoke the `getlogs` script). This script creates a `logs.jar` file in the root installation directory, and moves any existing copy of `logs.jar` to `oware\temp`. This jar compresses all logs necessary for troubleshooting. Read the jar yourself, or forward this file to technical support to help troubleshoot problems.

NOTE:

Server logs are in oware\jboss-x.x.x\server\oware\log. **Also:** If you install with an Oracle database, because the Oracle installation is outside OpenManage Network Manager's installer, OpenManage Network Manager does not create db_setup.log.

The `getlogs` script also gathers the tomcat web server logs for the web portal.

If `getlogs` halts, and does not produce a `logs.jar` file, it may be because someone installed this software, or a previous version as root, so `getlogs` does not have access to directories and groups owned by root. Change the permissions and/or ownership of those groups and directories to make `getlogs` work.

Increasing Startup Logging

For applications based on Oware 6.2.1 and later (see your `versions.txt` file or *Manage > Show Versions* for your version), you can add the following line to `oware\lib\pmstartup.dat`. If you add this line, this software logs all output from the startappserver script to a file:

```
server.out.filename=/opt/dorado/pmserver.log
server.out.filename=G:\Program Files\Dell EMC \OpenManage\pmserver.log
```

The destination you specify can be any valid path and file name. This helps when the server never starts or errors occur during deployment that would not be in the usual server.log.

Tuning Log Retention

The following properties are in `appserver.properties` and `redcell.properties` file for purging log files. As with all other properties, best practice is to override them in `owareapps/installprops/installed.properties`.

```
owappserver.properties
# This property defines how many days to retain server log files. All log
    files
# older than the specified retention days are purged. Back up older log
    files if
# you want to retain them. Set the property to -1 to disable this option.
    The
# default is 7.
oware.server.log.files.retention.days=7


redcell.properties
# This property defines where redcell client log files are stored The
# following is also the default:
redcell.log.files.location=oware.user.root/owareapps/redcell/logs
```

```
# This property defines how many days to retain the client's
# log files. Files older than the specified age are purged.
# Setting the property to a negative value disables log file deletion.
# The default is 7.
redcell.log.files.retention.days=7
```

Log Generation Fails with "Build Failed" Error (Linux)

Log generation and the build process fails when attempting to generate logs and is accompanied by an error like this:

```
BUILD FAILED
/opt/dorado/oware/conf/owrtbuild.xml:46: Problem creating jar: /opt/
    dorado/logs/ocpinstall_14332.log (Permission denied)
```

To successfully build logs, included files must be owned by the installing user (example: MyUser).

Solution: Locate and change the ownership of file(s) breaking the build process. To repair these, follow these steps:

1. Open a shell and source environment by typing `. /etc/.dsienv`.
2. Type `getlogs`.
3. Navigate to the file location(s) that appear in any error.
4. Type `ls -l` and review the owners for the files in this directory.
5. Type `su root` and enter root password.
6. Change the file ownership from user `root` (or other) to the installing user.

   Type, for example: chown `MyUser:MyUser ocpinstall_*` to change ownership of all files beginning with `ocpinstall_` .
7. Type `ls -l` to confirm new file ownership.
8. Type `exit` to return to the installing user prompt.
9. Repeat this process until getlogs builds a `logs.jar` successfully without error. You may need to correct file ownership in several locations before a successful build can occur.

To avoid a reoccurrence, do not perform any application-related command line operations while logged in as `root`. Such tasks must always be executed by the installing user.

WMI Troubleshooting Procedures

The following sections describe troubleshooting common WMI problems. To monitor with WMI, the following must be true:

- WMI must be enabled on the remote, monitored server and functioning properly.
- The remote server must be accessible through a Remote Procedure Call (RPC) connection to run WMI queries.

If your system does not meet these conditions WMI displays an *Unknown* status.

Examples of what may prevent the above can include the following:

- Not having local Administrator rights on the monitored host.
- Firewalls blocking the WMI traffic.
- An operating system not configured for WMI.
- An error in the credential password.

To help diagnose these issues, test the WMI services, the remote WMI connections, and you system's component configuration.

The following topics provide troubleshooting assistance:

- WMI Troubleshooting on the local host.
- Testing Remote WMI Connectivity
- Verify Administrator Credentials
- Enable Remote Procedure Call (RPC)
- Configure Distributed Component Object Model (DCOM) and User Account Control (UAC)
- Add a Windows Firewall Exception for Remote WMI Connections
- Checking the Authentication portlet to ensure correct credentials exist.

Finally, if these troubleshooting tips are not enough, see Additional WMI Troubleshooting on page 402.

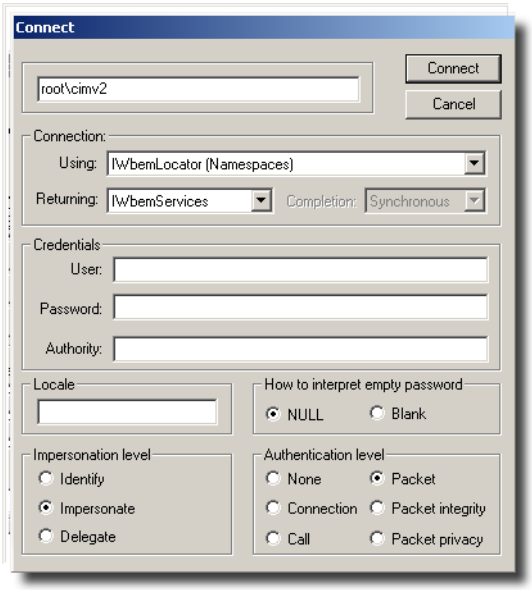
WMI and Operating Systems

Best practice is to avoid using Windows Vista And Windows 2008 for network monitoring of WMI. WMI works well Windows 7, even for larger networks. But with Vista and Window 2008 this is not true. Some tests even indicate that Windows 7 is up to 70 times faster than Windows 2008 or Vista. In these tests, hardware (CPU, memory) does not strongly affect WMI monitoring performance, nor does virtualization.

WMI Troubleshooting

To troubleshoot WMI, do the following:

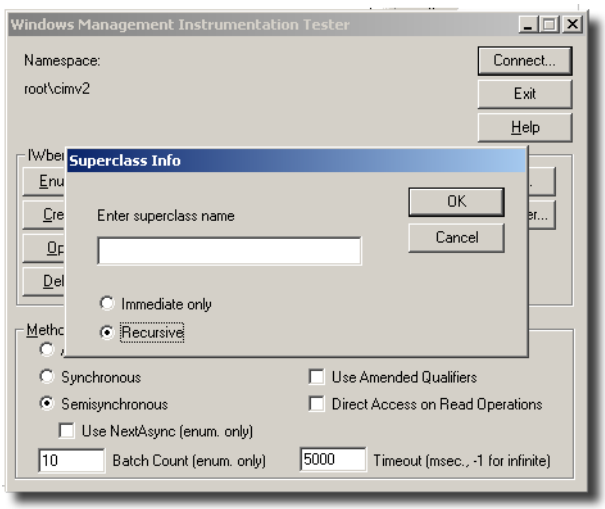
1. To test WMI locally, click *Start* > *Run*, then enter `wbemtest.exe` and then click *OK*. The `wbemtest.exe` program comes with Windows that supports WMI.
2. Click *Connect* on the Windows Management Instrumentation Tester window.
3. Enter `\root\cimv2` in the field at the top of the dialog box next to the *Connect* button.



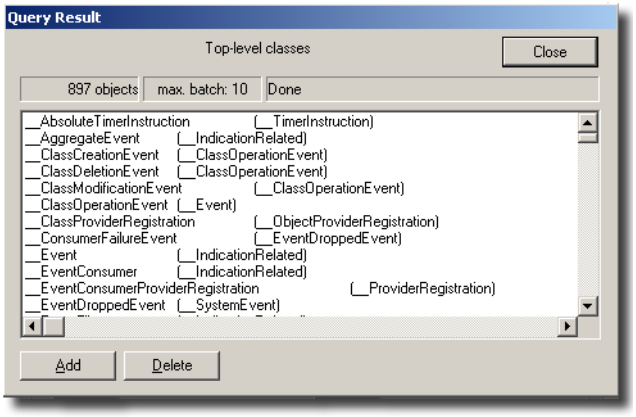
4 Click *Connect*.

5 Click the *Enum Classes* button.

6 Select the *Recursive* radio button. Leave the superclass name blank, and then click *OK*.



7 If the WMI classes you are querying appear in this list, local WMI services are functioning correctly.



8 If the list does not appear or does not contain the desired WMI class, WMI is not functioning correctly. Continue reading this section for guidance on repairing WMI services on the target server.

9 Click *Exit*.

10 If you did not see the desired classes, Reset the WMI Counters, and re-test until those classes appear.

Reset the WMI Counters

At times, the WMI performance counters may not get transferred to WMI because services were delayed or started out of order (see support.microsoft.com/kb/820847).

To manually reset the WMI counters:

1 Stop the Windows Management Instrumentation (WMI) service.

2 Open a shell (Click *Start* > *Run*, type `cmd`, and then click *OK*).

3 At the command prompt, type `winmgmt /resyncperf`, and then press [Enter].

4 At the command prompt, type `wmiadap.exe /f`, and then press [Enter].

5 Type `exit`, and then press [Enter] to close the command shell.

6 Restart the WMI service.

After resetting the WMI counters, retest WMI. If resetting the WMI counters did not solve your problem, see "WMI is Still Not Working, Now What?" on page 12.

Testing Remote WMI Connectivity

Ensure WMI is running on the remote, monitored host. This is similar to WMI Troubleshooting on the local host described above.

1 Click `Start > Run`, enter `wbemtest.exe` and then click *OK*.

2 Click *Connect* on the WMI Tester window.

3 Enter `\\Target_Primary_IP_Address\root\cimv2` in the field at the top of the dialog box. Replace *Target_Primary_IP_Address* in this entry with the actual host name or primary IP address of the target server.

4 Enter the appropriate administrator user name in the User field, the password in the Password field, and `NTLMDOMAIN:NameOfDomain` in the Authority field. Replace *NameOfDomain* with the domain of the user account specified in the User field.

5 Click *Connect*.

6 Click *Enum Classes*.

7 Select the Recursive radio button without entering a superclass name, and then click *OK*.

8 If the WMI class list appears, remote WMI is functioning correctly. Skip to the next topic and validate your credentials.

9 If the list does not appear, remote WMI is not functioning correctly. Continue reading this topic for guidance on restoring remote WMI connections on the target server, and retest remote WMI after completing each troubleshooting step.

11. Click the *Close* button, and then click *Exit*.

Verify Administrator Credentials

Only a credential that has administrator rights on the target server has the necessary permissions to access the target host's WMI services. Make sure that the username and password you are using belongs to an administrator on the target host.

If the administrator credential is a domain member, be sure to specify both the user name and the domain in standard Microsoft syntax. For example: `DOMAIN\Administrator`.

Enable Remote Procedure Call (RPC)

Remote WMI connections use RPC as a communications interface. If the RPC service is disabled on the target server, remote WMI connections cannot be established.

These steps show how to enable the RPC service:

1 Log on to the target host as an administrator.

2 Click *Start* > *Run*, then type `services.msc`, and then press [Enter].

3 Right-click Remote Procedure Call (RPC), and then click *Start* on the shortcut menu.

Configure Distributed Component Object Model (DCOM) and User Account Control (UAC)

If the target computer is running Windows Vista or Windows Server 2008, you may be required to make settings changes to allow remote WMI requests (See msdn.microsoft.com/enus/library/aa822854(VS.85).aspx).

DCOM—Edit Default and Limits permissions to allow the following actions:

- Local launch (default permission)
- Remote launch (default permission)
- Local activation (limits permission)
- Remote activation (limits permission)

For more information, see Enabling DCOM on page 399.

WMI Namespaces—Modify the CIMV2 security to enable and remote enable the account used to access the server or workstation through WMI. You must ensure the security change applies to the current namespace and subnamespaces. For more information, see Enabling Account Privileges in WMI on page 400.

User Account Control—Remote UAC access token filtering must be disabled when monitoring within a workgroup environment. For more information, see Disabling Remote User Account Control for Workgroups on page 401.

Enabling DCOM

WMI uses DCOM to communicate with monitored target computers. Therefore, for Application Performance Monitor to use WMI, you must have DCOM enabled and properly configured. Follow these steps to enable DCOM permissions for your Application Performance Monitor credentials:

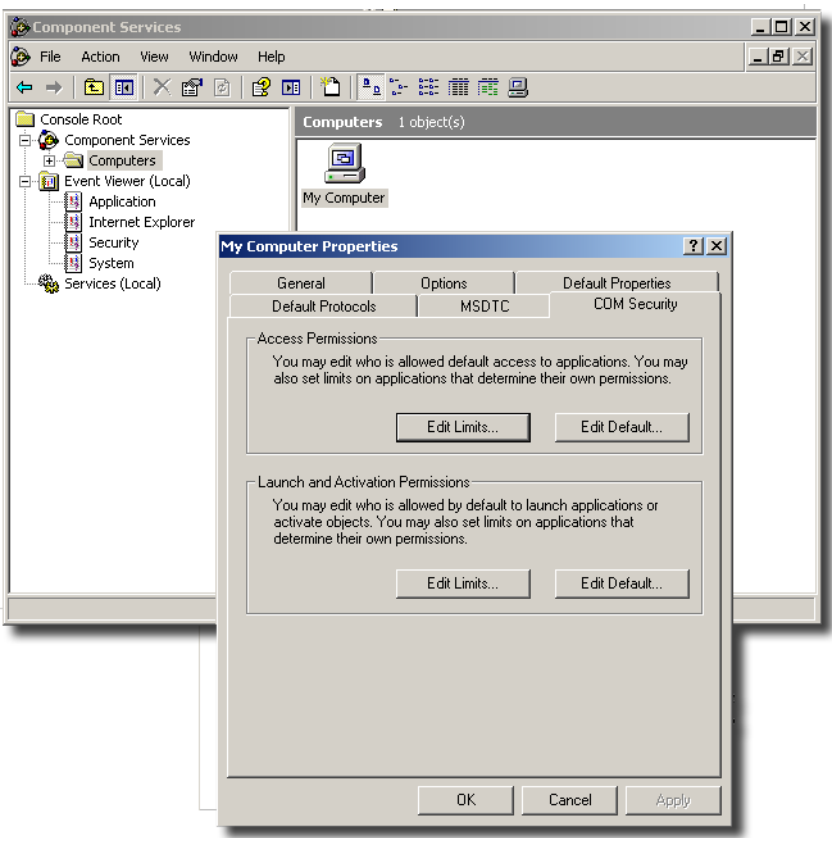
1 Log on to the target host as an administrator.

2 Navigate to *Start* > *Control Panel* > *Administrative Tools* > *Component Services*. (Only the Classic view of the Control Panel has this navigation path). You can also launch this console by double-clicking `comexp.msc` in the `/windows/system32` directory.

3 Expand *Component Services* > *Computers*.

4 Right-click *My Computer*, and then select *Properties*.

5 Select the COM Security tab, and then click *Edit Limits* in the Access Permissions grouping.



6 Ensure the user account collecting WMI statistics has *Local Access* and *Remote Access*, and then click *OK*.

7 Click *Edit Default*, and then confirm the user account collecting WMI statistics has *Local Access* and *Remote Access*, then click *OK*.

8 Click *Edit Limits* in the Launch and Activation Permissions grouping.

9 Ensure the user account collecting WMI statistics has *Local Launch*, *Remote Launch*, *Local Activation*, and *Remote Activation* enabled, and then click *OK*.

10 Click *Edit Default*, and then ensure the user account collecting WMI statistics has *Local Launch*, *Remote Launch*, *Local Activation*, and *Remote Activation* enabled.

11 Click *OK*.

Enabling Account Privileges in WMI

The account you specify for authentication must possess security access to the namespace and subnamespaces of any monitored target hosts. To enable these privileges, complete the following procedure.

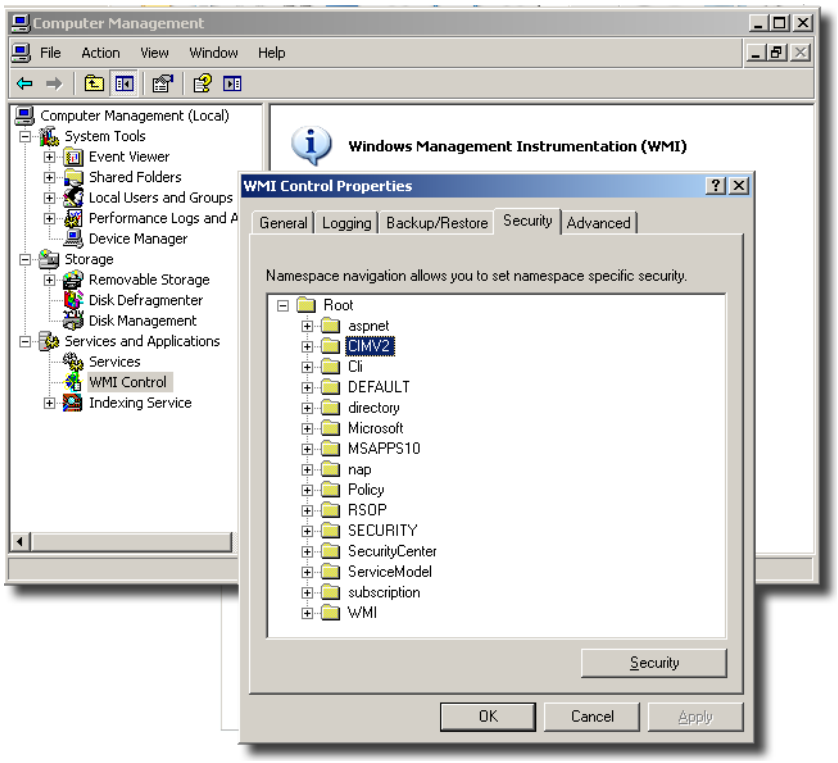
To enable namespace and subnamespaces privileges:

1 Log on to the host you are monitoring as an administrator.

2 Navigate to *Start* > *Control Panel* > *Administrative Tools* > *Computer Management* > *Services and Applications*. (Classic View of the Control Panel this navigation path).

3 Click WMI Control, and then right-click and select Properties.

4 Select the Security tab, and then expand Root and click CIMV2.



5 Click Security and then select the user account used to access this computer and grant the following permissions:

–Enable Account

–Remote Enable

6 Click *Advanced*, and then select the user account that accesses this computer.

7 Click *Edit*, select *This namespace and subnamespaces* in the *Apply to* field, and then click *OK*.

8 Click *OK* on the *Advanced Security Settings for CIMV2* window.

9 Click *OK* on the *Security for Root\CIMV2* window.

10 Click *Services* in the left navigation pane of *Computer Management*.

11 Select *Windows Management Instrumentation* in the *Services* result pane, and then click *Restart*.

Disabling Remote User Account Control for Workgroups

If you are monitoring a target in a workgroup, you must disable remote User Account Control (UAC). Although this is not recommended, it is necessary when monitoring a workgroup computer. Disabling remote user account control does not disable local user account control functionality.

△ CAUTION:

The following modifies or creates a registry key. Changing the registry can have adverse effects on your computer and may result in an unbootable system. Best practice is to back up your registry before making these changes.

To disable remote UAC for a workgroup computer:

1 Log on to the host you want to monitor as an administrator.

2 Click Start > Run, and enter `regedit`.

3 Expand `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`.

4 Locate or create a DWORD entry named LocalAccountTokenFilterPolicy and provide a DWORD value of 1.

NOTE:

To re-enable remote UAC, change the DWORD value to 0.

Add a Windows Firewall Exception for Remote WMI Connections

If the target computer has Windows Firewall enabled, it must have a Remote WMI exception to allow remote WMI traffic through (See /msdn.microsoft.com/en-us/library/aa389286(VS.85).aspx). Follow these steps to add this exception:

1 Open a command shell (Click *Start* > *Run*, type `cmd` and then press [Enter]).

2 At the command prompt, type

```
netsh firewall set service RemoteAdmin enable
```

Press [Enter]

3 Type `exit` then press [Enter].

If adding the firewall exception did not solve your problem, see Additional WMI Troubleshooting below.

WMI Authentication

If the above troubleshooting has been done correctly, ensure the authentication credentials for the WMI device in *Resources* match those for an administrator. Select the device in the Resources screen, and click *action* > *Open* (or right-click and select *Open*). Go to the *Authentication* node of the tree, and confirm that the correct authentication objects appear there.

Additional WMI Troubleshooting

The above discusses the most common errors behind WMI failures. After trying these, if you are unable to get WMI services working, consult the following articles about this subject on Microsoft's Technet and Developer Networks:

- *WMI Isn't Working!: Troubleshooting Problems with WMI Scripts and the WMI Service.* (See www.microsoft.com/technet/scriptcenter/topics/help/wmi.mspx)
- *WMI Diagnosis Utility: A New Utility for Diagnosing and Repairing Problems with the WMI Service* (See www.microsoft.com/technet/scriptcenter/topics/help/wmidiag.mspx)
- *WMI Troubleshooting* (See msdn.microsoft.com/enus/library/aa394603.aspx)

NOTE:

While the above URLs are believed correct, they may change.

jstack Debugging in Windows 7

Technical assistance sometimes uses the jstack stack trace tool to debug problems in this software. When you install application server to run as a service (autostart), the user SYSTEM owns the application server process. You also cannot log into Windows 7 as user SYSTEM. For security's sake, no other user can access a service running as the SYSTEM user in later Windows 7 kernels. The jstack tool therefore does not work if you run it as the (non-SYSTEM) user logged in to Windows 7.

Workaround: To view a jstack output for application server, or any service (and its subprocesses) running as the user SYSTEM, you must run jstack (and jps) as user SYSTEM. Windows 7 provides no direct way to log in as user SYSTEM, so the following sidesteps this prohibition:

1. Open a command shell (Click the *Start* icon and type `cmd` in the *Search Programs and Files* field.)
2. At the command prompt, type:

   ```
   sc create testsvc binpath= "cmd /K start" type= own type= interact
   ```
3. Then type:

   ```
   sc start testsvc
   ```
   The `sc start` command immediately creates a new command shell owned by SYSTEM, even if the original command window failed to start with error 1053 (this is expected since `cmd.exe` does not have any service-related code in it).
4. Open an oware shell inside the SYSTEM-owned command prompt created in Step 3. (Type `oware` at the command line.)
5. In that oware shell, run `jps` to see the process ID (PID) of the application server's Java process (`OWLaunchV2`).
6. Then run `jstack [PID]` in the SYSTEM shell.
7. To delete the testsvc when you are finished, type this on a command line:

   ```
   sc delete testsvc
   ```

FAQs about Monitoring Mediation Servers

After making a UDP-based JGroups discovery request and receiving a response from an application server in the cluster, each mediation server makes an RMI (TCP) call to an application server every 30 seconds. This RMI call results in a "call on cluster" on the application server cluster, using JGroups (UDP by default), to call the agentHeartbeat method of the OWMedServerTrackerMBean on each application server in the cluster. The primary application server updates the timestamp for the medserver in question, and the others ignore the call. Every five seconds, the primary application server checks to see if it has not received a call from a mediation server in the last 52 seconds. If it has not, it attempts to verify down status by pinging the suspected mediation server. Then it issues an RMI call on that mediation server. It considers the meditation server down if the ping or the final RMI call fails. This avoids false meditation server down notifications when a network cable is pulled from an application server.

- Does the application server wait 15 seconds after receiving the mediation server's response? Or does it monitor mediation server every 15 seconds regardless of the mediation server's response?

  The receipt of the mediation server's RMI call is on a different thread than the monitoring code. The monitoring code should run every 5 seconds, regardless of the frequency of

mediation server calls. However, after investigating the scheduling mechanism used (the JBoss scheduler - http://community.jboss.org/wiki/scheduler), it is possible that other tasks using this scheduler could impact the schedule because of a change in the JDK timer implementation after JDK 1.4.

- What kind of functionality (JMS?) does application server use to send and receive OpenManage Network Manager messages?

  The application server does not actively monitor the mediation servers unless it fails to get a call from one for 52 seconds. If it does try to verify a downed mediation server, it uses an RMI call.

  The RMI calls use TCP sockets. It may use multiple ports: 1103/1123 (UDP - JGroups Discovery), 4445/4446 (TCP - RMI Object), 1098/1099 (TCP - JNDI), or 3100/3200 (TCP - HAJNDI), 8093 (UIL2).

- What kind of problem or bug would it make application server to falsely detect a mediation server down? For example, would failing to allocate memory cause application server to think a mediation server is down (dead)?

  An out of memory error on an application server could result in a false detection of a downed medserver.

- If such memory depletion occurs as described in the previous answer, would the record appears in the log? If it doesn't appear in the log, would it possibly appear if the log-level is changed?

  An out of memory error usually appears in the log without modifying logging configuration, since it is logged at ERROR level.

- The log shows that a mediation server was detached from the cluster configuration, but what kind of logic is used to decide the detachment from the cluster? For instance, would it detach application servers if they detect the mediation server down?

  JBoss (JGroups) has a somewhat complex mechanism for detecting a slow server in a cluster, which can result in a server being "shunned." This logic remains, even though we have never observed the shunning of a server resulting in a workable cluster. This is the only mechanism which automates removing servers from the cluster. The configuration for this service is located in `$OWARE_USER_ROOT/oware/jboss-x.x.x/owareconf/cluster-service.xml`. Shunning can be disabled by replacing all `shun='true'` instances with `shun="false"`. A flow control option also exists which regulates the rate of cluster communication to compensate for one server being slower in processing cluster requests than another. The detection of a mediation server being down with the heartbeat mechanism described here does not attempt to remove the medserver from its cluster.

- Why does Mediation server not appear in the control panel?

  Make sure you have followed the instructions in the *Installation Guide*.

Linux Issues

The following are issues with Linux installations:

- Install in `/opt/dorado`, unzip package in, for example, `/opt/installs`, not `/opt/dorado`.
- Linux (executed as the root user) uses this command:

  ```
  /etc/init.d/owaredb start
  ```

  You should see the following response in the shell where you execute this command:

```
Starting MySQL[  OK  ]
```

- If you experience problems with discovery, and see errors on startup similar to the following:

```
[com.dorado.core.mediation.snmp.SRSnmpEventReportDispatcher] (Thread-36
    RecvTrap Exception :
com.dorado.core.mediation.snmp.SRSnmpException:
at com.dorado.core.mediation.snmp.SRSnmpSession.nRecvTrap(Native Method)
at
    com.dorado.core.mediation.snmp.SRSnmpSession.recvTrap(SRSnmpSession.ja
    va:733)
at
    com.dorado.core.mediation.snmp.SRSnmpEventReportDispatcher.run(SRSnmpE
    ventReportDispatcher.java:96)
at java.lang.Thread.run(Thread.java:662)
```

or

```
ERROR [com.dorado.core.mediation.syslog.OWSysLogListener]
    (OWSysLog.Listener Received a null SysLog message. SysLog port may be
    in use. Shutting down SysLog listener.
```

You may be able to solve this issue by increasing the available memory on the entire system or lowering the heap memory used by your system. The former option is best practice.

Application Server Memory (Linux and Windows)

I. Linux application server appears to have low memory.

Solution: Memory statistics using TOP can be deceiving. Linux may have borrowed some free memory for disk caching. To determine if this is the case:

1 Open a shell and execute command: `free -m`

This returns the amount of (true) free/available memory for application use in megabytes. See cache value in line `-/+ buffers/cache: 26441 37973` below…

```
[redcell@AppRedcell01 ~]$ free -m
total used free shared buffers cached
Mem: 64414 63823 590 0 364 37018
-/+ buffers/cache: 26441 37973
Swap: 65535 11 65524
[redcell@AppRedcell01 ~]$
```

Here, 37,973M is still free for application use.

See www.linuxatemyram.com/ for more detail on this topic.

Alternatively,

2 If TOP reveals an excessive and abnormally high memory usage for the application java process, you may need to restart your application server and evaluate installed/available memory with regard to your sizing and application usage requirements. Install more server memory as needed.

II. Genuine memory issues appear if logs contain an error like `java.lang.OutOfMemoryError: GC overhead limit exceeded`, and application server performance is slow, possibly preventing log into web portal. You may also see many other errors, for example, from performance monitoring:

```
WARN  [com.dorado.broadscope.polling.PollingResultsDAOImpl]
    (WorkManager(2)-99:) Low on memory.  Discarding this batch.
```

Solution: These errors indicate memory resources are low or have been depleted.

To address this, first review any potential causes for an increase in memory usage. For example, has there been a significant increase in performance monitor load, perhaps from reducing polling times or an increase in targets/attributes? Have there been any other changes?

Assuming sufficient server memory is available, increase heap size. Adjust memory values below according to your environment and configuration needs:

1 Shut down the application.

2 Open `owareapps/installprops/lib/installed.properties` file for editing.

3 Modify the `oware.server.max.heap.size` property

```
oware.server.max.heap.size=3072m
```

In this example, a recommended increase would be 25% to 4096m.

4 Increase `oware.server.min.heap.size` to match (4096m)

5 Save changes to `installed.properties`.

6 Restart the application.

NOTE:

Heap adjustments work for Windows too.

III. Out of Memory errors like `Out of Memory: unable to create new native thread` in logs for server (application or mediation) may indicate memory resources are sufficient, but threads are not.

Solution: The operating system may be limiting the number of available threads for use by the application. Check/modify the `ulimits` settings with these steps:

1 Open shell/CLI and type `ulimits -a`.

Open files and User Processes should not be set to typical defaults (1024). Change these with the next steps.

2 Open `/etc/security/ limits.conf` for editing.

3 Add the following lines and save.

```
<installing user> soft nofile 65536
<installing user> hard nofile 65536
<installing user> soft nproc 65536
<installing user> hard nproc 65536
```

4 Restart the application processes.

Refer to the *OpenManage Network Manager Installation Guide* for Linux installation and upgrade instructions and best practices.

Linux syslog not displaying

Application does not display syslog messages.

On Linux based platforms, under certain circumstances, a race condition at application startup may impact syslog event/messaging functionality. If syslog messages are not displaying as expected, please apply the following **workaround** to restore functionality.

1) Shutdown the webserver.

2) Restart the appserver.

3) Start the webserver after the appserver's status shows 'ready'.

This process may need to be repeated if the server is restarted.

HA installation issue on Linux

In version OMNM 6.2, servers within HA system will fail on startup caused by the following exception:

ERROR [org.jgroups.protocols.UDP] (Timer-1,192.168.54.41:37377:) failed sending message to null (69 bytes)

The recommended workaround is to modify a line with the run.sh script found in install_path/oware/jboss-5.1/bin

From

JAVA_OPTS="$JAVA_OPTS -Djava.net.preferIPv4Stack=false"

To

JAVA_OPTS="$JAVA_OPTS -Djava.net.preferIPv4Stack=true"

Servers restart is required.

Linux HA does not support IPv6 as default.

While IPv6 is supported on Windows HA, Linux HA does not support IPv6 as default. To acquire IPv6 on Linux HA, it's suggested that users must follow these steps enable unicast within the Mediation cluster. Apply the configuration changes to all Mediation servers.

1. Add the property oware.unicast=true to installed.properties file located in .../dorado/owareapps/installprops/lib directory.
2. Locate .../oware/jboss/server/oware/deploy/cluster/jgroupschannelfactory.sar/META-INF/jgroups-channelfactory-stacks.xml.
3. In the TCP section (you can search by <stack name="tcp"), comment this portion:

   <!--Alternative 1: multicast-based automatic discovery. -->

   <MPING timeout="3000"

   num_initial_members="3"

   mcast_addr="${jboss.partition.udpGroup:230.11.11.11}"

   mcast_port="${jgroups.tcp.mping_mcast_port:45700}"

   ip_ttl="${jgroups.udp.ip_ttl:2}"/>
4. And Uncomment

   <!-- Alternative 2: non multicast-based replacement for MPING. Requires

   a static configuration of all possible cluster members.>

   <TCPPING timeout="3000"

   initial_hosts="${jgroups.tcpping.initial_hosts:localhost[7600],localhost[7601]}"

   port_range="1"

num_initial_members="3"/-->

CAUTION:

Make sure you modify stack "tcp" section, not "tcp-sync" section

Example:

<!--Alternative 1: multicast-based automatic discovery.

<MPING timeout="3000"

num_initial_members="3"

mcast_addr="${jboss.partition.udpGroup:230.11.11.11}"

mcast_port="${jgroups.tcp.mping_mcast_port:45700}"

ip_ttl="${jgroups.udp.ip_ttl:2}"/>

-->

Alternative 2: non multicast-based replacement for MPING. Requires

a static configuration of all possible cluster members.>

<TCPPING timeout="3000"

initial_hosts="${jgroups.tcpping.initial_hosts:10.35.35.200[7600],10.35.35.201[7601]}"

port_range="1"

num_initial_members="3"/

Where 10.35.35.200 and 10.35.35.201 are IPaddresses of Mediation servers.

5 Restart Mediation servers. (#service oware stop/start)

Device Prerequisites

Often, devices require pre-configuration before they are manage-able by this software. For example, the management system application server must have access to the device, and often must be listed on the access control list for the managed device.

Common Device Prerequisites

The following are common prerequisites:

Credentials—WBEM credentials have a role in discovering the device. Your system must have access to the computer using Administrative only credentials. These are the same credentials as the user installing WBEM on the device.

Telnet / SSH credentials are necessary for other supported applications.

For full functionality, this WBEM device driver requires administrative (root) access. Many devices may only allow root logins on a local console.

In such cases, configure the Telnet/SSH authentication for these devices to login as a non-root user—and, in Authentication Manager, enter `su` in the *Enable User ID* field and enter the root

user's password in *Enable User Password* in that same authentication. This enables full device management functionality with root access.

NOTE:

Credentials for Telnet / SSH should have a privilege level sufficient to stop services and to restart the computer system.

Firewall—Some firewalls installed on the computer may block Web-Based Enterprise Management requests. Allow those you want to manage.

License—Make sure you have the correct WBEM driver license installed. Licenses come in the following types:

- Major Vendor by Name - Such as Dell, Compaq, HP, Gateway.
- Server/Desktop individual license support.
- Generic computers - non-major vendors.
- ALL - this gives the driver all capabilities for any computer system.

Aruba Devices

By default, only SSH interactions work on these devices. If you want to use telnet you have to configure the device through the console or through an SSH session and turn it on.

Cut through or direct access sessions are only supported for SSHv2. You must create an SSHv2 management interface for the device and use it when attempting direct access. If you use SSHv1 the session does not connect (the ArubaOS does not support SSHv1), and if you select telnet, the driver cannot log into the device automatically, and must login manually.

SNMP v2c only supports read operations, not write. SNMP v3 supports both read and write, but not SNMP v3 informs. To manage Aruba devices you must use SNMP v2 or v3. Up to Aruba OS3.1.1.2, SNMPv2c (read-only) and v3 (read-write) are recommended. SNMP v1 does not work correctly.

NOTE:

Although SNMP handles the bulk of the communication with this device, and you must supply the correct SNMP authentication information, some information comes through telnet interaction, so you must supply telnet/SSH authentication too for all device interactions to work correctly.

Backup and Restore

You can backup or restore text files that reflect the *Startup Config*, and *Running Config* as well as backup/restore of a binary *Flash* memory for the selected device. You can compare, store, view and version the text files, and can restore either text or flash memory to the device if you have the File Management option installed.

Because the Aruba mobility controller's flash memory backup is a compressed, binary `.tar.gz` file, the displayed Current Config is not always textual. The flash file is binary, so you cannot view it as text. Nevertheless, you can restore it as long as the backup file has the extension of `.tar.gz` Using this application to backup the flash automatically creates the file with this extension.

Avaya Device Prerequisites

You must do the following for the device driver to function correctly with Avaya devices. Whether you use RTCP or not, do the bullet point setup steps outlined in Setting Up RTCP on page 410, below.

Cut-Through

Avaya Communication Manager uses a special port for telnet sessions. To use the Telnet Cut-thru feature in this software, you must modify the port. You can do this during the discovery process by creating a Telnet authentication object and entering port 5023. Alternatively, once you install Communication Manager, open it from the Resources screen, select the Authentication tab and create a new Telnet management interface with port 5023. When you initiate a Telnet cut-thru session, Customer Manager asks for an emulation type. Select type 4410.

Setting Up RTCP

The following describes setting up RTCP with Avaya devices. Do this on the Avaya Media Server with the Media Server's Management Web Interface using a browser (for example, Internet Explorer) to access the IP address of the media server. For an S8300, S8400, S8500 use the server's IP address. For the S87xx, use the active server IP address—not server A or server B but the active server address. When accessing the web manager, after logging in, navigate to the Maintenance Web Page to see the following menu choice:.

NOTE:

When changing SNMP settings Avaya recommends stopping and restarting the agent.

- Enable SNMP v2 on the device (under *Alarms* > *SNMP Traps*)
- Ensure the SNMP community strings match on the authentications you have configured and on the device (*Alarms* > *SNMP Agents*).
- Mediation Server (or Application Server, if enabled as a Mediation Server) must be allowed access on the device, either through its specific IP address(es) or by checking *Any IP address* under *Alarms* > *SNMP* Agents.
- *Security* > *Firewall* must have *SNMP, HTTP* and/or *HTTPS*, and *Telnet* and/or *SSH* and *RTCP* enabled both as *Input* and *Output* from the Server. If your system collects SNMP Traps and syslog messages, select those for Output from Server only.
- You must confirm, or start, the SNMP agent (Master Agent) on the device under *Alarms* > *Agent Status*.

After modifying the alarm and security areas of the web manager, you need to access the *Communication Manager* command line interface (CLI) using telnet, the *Native Configuration Manager* (from the main web management page) or use Avaya's *Site Administration* software. If telnetting to the CLI, choose the `w2ktt` terminal type upon login. You must have a Communication Manager login which may or may not be the same as the web manager login and password.

Execute and change the following:

1 Change **system-parameter ip-options** and specify under RTCP Monitor Server the:
   - Default server IP address = the Application server IP address
   - Default port = Must match what you put in your software
   - Default RTCP Report Period = you can leave at default

- Enter/submit the changes

```
display system-parameters ip-options                          Page 1 of x

                    IP-OPTIONS SYSTEM PARAMETERS

 IP MEDIA PACKET PERFORMANCE THRESHOLDS
    Roundtrip Propagation Delay (ms)     High: 800      Low: 400
                   Packet Loss (%)       High: 40       Low: 15
                   Ping Test Interval (sec): 20
    Number of Pings Per Measurement Interval: 10

 RTCP MONITOR SERVER
                  Default Server IP Address:
                        Default Server Port: 5005
           Default RTCP Report Period(secs): 5

AUTOMATIC TRACE ROUTE ON
           Link Failure? y


 H.248 MEDIA GATEWAY                 H.323. IP ENDPOINT
 Link Loss Delay Timer (min):5       Link Loss Delay Timer (min):
                                       Primary Search Time (sec):
                                Periodic Registration Timer (min):
```

2 Change **ip-network-region x** (for every network region that pulls RTCP information)

- On page one, make sure that RTCP Reporting is enabled.
- Under RTCP monitor server Parameters,

  –Use default server parameters (this uses the parameters you set up on the `system-parameter ip-options` form)

  –If you want to specify a separate server IP address, specify it under server IP address and server port

  –Enter/submit the changes.

```
change ip-network-region n                                    Page 1 of x
                              IP NETWORK REGION
  Region: n
Location:                  Authoritative Domain:
    Name:
                             Intra-region IP-IP Direct Audio: n
MEDIA PARAMETERS             Inter-region IP-IP Direct Audio: n
   Codec Set: 1                       IP Audio Hairpinning? n
UDP Port Min: 2048
UDP Port Max: 3029                  RTCP Reporting Enabled? y
                           RTCP MONITOR SERVER PARAMETERS
DIFFSERV/TOS PARAMETERS    Use Default Server Parameters? y
 Call Control PHB Value:                 Server IP Address:    .   .   .
        Audio PHB Value:                       Server Port: 5005
        Video PHB Value:

802.1P/Q PARAMETERS                RTCP Report Period(secs): 5
 Call Control 802.1p Priority: 7
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 7
                                  AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                   RSVP Enabled? y
  H.323 Link Bounce Recovery? y             RSVP Refresh Rate(secs): 15
 Idle Traffic Interval (sec): 20         Retry upon RSVP Failure Enabled? y
   Keep-Alive Interval (sec): 6                        RSVP Profile:
            Keep-Alive Count: 5          RSVP unreserved (BBE) PHB Value: 40
```

Brocade Devices

This software will not telnet connect to some devices if they use the factory default password. You must set the password to something other than that default. This software does not recognize the additional prompt asking that default password be changed each time login occurs.

Follow these steps and update firmware on the non-RX devices:

1 Download the firmware update (.zip file) from www.brocade.com

2 Extract that zip file to the download directory of the External FTP file server your system uses.

3 Create an empty file named `release.plist` and load into the OS Image manager portlet.

4 Deploy that image, selecting the device and `release.plist` file loaded in your system. To deploy the image, select the device(s) and select the `release.plist` file in OS Manager.

5 Remove any remaining files before attempting the next Brocade firmware update.

NOTE:

You cannot deploy these updates using this software's internal FTP server.

For RX devices, download and deploy firmware updates as you ordinarily would, registering the OS image in the OS Images manager (see the *OS Images* section of this guide), and deploying it to either a device or group with the *action* menu.

BIG-IP F5

OpenManage Network Manager supports the BIG-IP F5 load-balancing appliance and software. It supports the following capabilities, and requires the listed device configurations:

- SNMP—This requires adding the IP address from which you manage the F5 to its Client Allow List under System -> SNMP -> Agent -> Configuration). Supports SNMP-based default device/resync using the ifTable - creates interface sub-components.
- Event Management—SNMP Trap Definitions (Tip: search for event definitions beginning with "big").
- Reports—Run any default OpenManage Network Manager reports against F5 inventory.

Features not supported

- Any CLI-based functionality (NetRestore, CLI Cut-Thru, and so on)
- Link Discovery
- Port creation

Cisco Devices

The following sections discuss prerequisites and limitations of Cisco device management capabilities.

Setup Prerequisites

You must include the *Enable* user ID. Omitted enable user IDs may interfere with correct device management.

You must create Authentication objects for Cisco Switches with an Enable user and password. Otherwise authentication for Interface level DC login sessions fail. The Cisco Router authentication rules automatically send the Enable user/password at the interface level.

For IOS devices, access to various system command modes on the device may be defined by specifying an access privilege level for a user account. Access privilege level 15 is required to access Enable (privileged) mode. This software requires the user account for authenticating with and managing a device has a privilege level of 15.

Ensure that user accounts associated with CLI Authentication objects in your system are configured on the device with privilege level 15. Consult your device's manuals for additional information about configuring this privilege level.

CAUTION:

If you upgrade IOS when you have not copied running-config to Startup-config, provisioning services may fail because of the unexpected device error message below. This message causes "write memory" command to fail. In the application the user may see a message like "failure to terminate telnet session" Device message: *Warning: Attempting to overwrite an NVRAM configuration previously written by a different version of the system image.* **Also:** Currently unsupported: Chassis View, Discrete configuration.

Saving Running-Config to Startup Config

To save the running-config to startup-config whenever the router's configuration is updated uncomment the following in cisco.properties to enable this feature.

```
#cisco.ios.save.running.config=true
```

This copying behavior should not be fatal to the configuration that was updated but a job message displays the failure or success.

NOTE:

Nexus configuration restore to start-up is not supported. When you attempt this, an error including `This command is deprecated` appears on 3000 series devices. On 5000 series, the error is `sysmgr_copy_nvram_dest_action: src uri_type = 1 is not supported yet`. (25242)

Copying to the Device Rather than Your System

You can have backup copy running configurations to the device's disk rather than the system's database. This requires no intervention of FTP since everything occurs on the device itself. The option appears when you change the following properties in the cisco.properties file in `owareapps/cisco/lib`:

```
#flags that enable direct copy run start
cisco.rmc.save.config=false
cisco.backup.save.config=false
```

When these are *true* you can back up running-config to startup-config for Cisco devices. You can select this option in addition to standard backup in the backup configuration screen (choose *running-config* from the File System pick list, and *startup-config* from the File Server Protocol pick list.) You can also trigger it from the *System* > *General* screen's *Save Config* button.

Adaptive CLI FAQs

- Why share an existing schema from another Adaptive CLI (ACLI) versus creating a new one with each ACLI?

  One reason to use the same schema is to accommodate a complementary ACLIs. For example one ACLI creates an entity and you want a script to remove the same entity. For such examples, the valid values, labels, and so on, for the attributes are always going to be the same in your create and delete ACLIs. Therefore, it is safest to use the same single referenced version of the Schema. You can share the same schema, and your delete script can mark the attributes it does not use as *Not applicable*.

- What is the best practice for exporting ACLIs to import later into another system?

  If you have ACLIs that you need to export so that you can import them into a production system, then the recommended practice is to create a separate file for each ACLI and export them one at a time.

You can group select multiple ACLIs in the Adaptive CLI Manager and export them to a single file, but this can be difficult to maintain if changes are being made frequently to the ACLIs. Best practice is that only ACLIs directly sharing a common Schema (example a Create ACLI and its complimentary Delete ACLI) be exported to the same file. Keep in mind how to maintain/version/update the ACLIs and associated shared schemas when plotting how to map your export files, and frequently back up your export files to external devices/machines. You can use source control systems version/maintain ACLI export files, since they are in XML format.

- If I change an ACLI's schema shared by other ACLIs, do I need to do anything to the other ACLIs?
  If you have multiple ACLIs sharing the same Schema, you should be in the habit of retesting the other ACLIs using that schema for to ensure no unintended side effects occur.

NOTICE

Regularly export all ACLIs with the same schema before modifying the schema by editing any of the ACLIs that use it. **Also:** Test your ACLI scripts in a telnet or direct access session with the target device(s).

NOTICE

When previewing ACLI and preview form is empty, most likely Perl is not installed. Best practice is to use Perl version 5.10 or later (however not 5.16).

Server Information

You can see mediation and application server information in JMX Console. The URLs for this console:

- **Mediation Server JMX**: http://[mediation server IP address]:8089/jmx-console/ (for stand-alone mediation servers), or port 8489 for HTTPS.
- **Application Server JMX**: http://[application server IP address]:8089/jmx-console/, or port 8489 for HTTPS.

Some information visible in these consoles:

Is a mediation server active or standby?—Open the JMX console for the mediation server, then click PollingEngine and view the *Active* attribute. If *true* the mediation server is primary, if *false* it is standby.

To which application server is mediation server posting data?—In the mediation server's console, click ClusterPrimaryDesignator and then view the AppServerPartitionName attribute.

List active subscriptions and targets—Click PollingEngine, then invoke the getSubscriptionAndTargetInfo operation.

Is mediation server writing polling results to the spool file?—Click MonitorPollingHandlerMBean and then view the DataBeingWrittenToSpoolFile attribute. While there you can also see the most recent time the mediation server posted data to the application server (item 7) by viewing the MostRecentPostTime attribute.

When does a server skip execution and what is the total number of skips?—Click PollingEngine and then viewing those attributes. While there, you can also see the last time the server rejected execution and the last time that happened

NOTE:

The jmx-console is a Development tool used for troubleshooting and not accessible to the application user. Please request assistance through Dell EMC support channels to investigate any potential application issues..

Environment / Operating System Issues

The following are items that have historically caused some problems. They may not apply to your environment.

CRON Events

CRON events can update Linux Releases, check for linkage errors and run through other tasks. This should occur when server traffic is generally higher. If necessary, change it to run late during off peak hours.

Potential Problem Processes

auditd—This process logs errors periodically, and can send RESTART or KILL signals to processes outside of its policies. This could be dangerous if configured wrong.

cpuspeed—Throttles down CPU speeds within the Kernel. Since OpenManage Network Manager's Java runs in a VM it is unaware of sudden increase/decrease in CPU speeds, and this could pose issues in threading and calculating thread counts.

SELINUX

This should be disabled. To check, run the following:

```
[root@AppRedcell01 bin]# selinuxenabled && echo enabled || echo disabled
```

To fix this, if it indicates it is enabled, modify the `/etc/selinux/config` and change `targeted` to `none` so this is preserved on reboots.

Hardware Errors

A fragment found in `dmesg`, triggered further investigation. This detected memory errors.

```
[Hardware Error]: Machine check events logged
Errors found in /var/log/mcelog:
Hardware event. This is not a software error.
MCE 0
CPU 30 BANK 9
TIME 1370474184 Wed Jun  5 17:16:24 2013
MCA: MEMORY CONTROLLER GEN_CHANNELunspecified_ERR
Transaction: Generic undefined request
STATUS 900000400009008f MCGSTATUS 0
MCGCAP 1000c18 APICID c0 SOCKETID 3
CPUID Vendor Intel Family 6 Model 47
```

DNS Does Not Resolve Public Addresses

DNS must permit application servers to resolve public DNS names like google.com. Web server needs this to determine its public facing interface by determining which route the packet went out on quick test.

Raise User Limits

If User Limits are low on the Application Servers and possibly Mediation Servers, these can impact threading and normal server behaviors.

Web Server

The memory configuration (heap min/max) should also be the same for all server environments.

Portal Memory Settings

To manually change the web portal heap settings, change the `setenv.sh` (Linux) or `setenv.bat` (Windows) file:

```
set "PORTAL_PERMGEN=512m"
set "PORTAL_MAX_MEM=3072m"
set "PORTAL_INIT_MEM=768m"
set "PORTAL_32BIT_MAX_MEM=768m"
```

These files are in the `Tomcat***/bin` directory. For Linux, restart the portal service to apply new memory settings. In Windows, besides updating `setenv.bat` you must run `service.bat update` in that same directory.

You can increase these to even higher figures if your system has the memory available.

NOTICE

Make sure only one Tomcat process is running, otherwise your web server may exhibit poor performance.

Post Upgrade Web Portal Problems

After applying patches, restarting processes or other recent activity, web portal exhibits undesired behavior like the following:

- Displaying pink bar in application portlets indicating applications are `temporarily unavailable`.
- Message in application portlets indicating `resource unavailable`.
- Actions screen does not appear after right-click device and choosing *Actions*.
- Inability to expand containers or previously selected container expands when clicking another container.

Solution: These, and other symptoms, can stem from browser caching or attempting to login too soon after starting the application. To resolve, try waiting and/or clearing the browser cache.

Clustering

You must enable Clustering on multiple web servers, otherwise index and users become out of sync. To solve this: enable clustering on the web servers by turning on cluster properties found within `synergy/conf/server-overrides.properties`

Upgrade Installations

The following outlines tasks to execute when you are updating your drivers, extensions or license. Refer to Upgrade / Data Migration Fails on page 382, Post Upgrade Web Portal Problems on page 416 for instructions about how to prevent and/or handle upgrade problems that can occur.

Patch Installation

Updating Driver Patches

1. Shut down your system.
2. On the application server designated as `oware.config.server` in `[installation root]/owareapps\installprops\lib\installed.properties`, copy the update file with the `ocp` or `ddp` extension to the `owareapps` directory.
3. Open a shell or command prompt, and Source the oware environment (Windows: `oware`. Linux: `. /etc/.dsienv`), and execute the following command lines:
4. `cd $OWAREAPPS`
5. `ocpinstall -x <ocp/ddp filename>`
6. `ocpinstall -u <ocp/ddp filename>`
7. ocpinstall -s <ocp/ddp filename>

Repeat steps 1 - 5 on any secondary application or mediation servers.

Adding or Updating Extensions

1. Copy extensions to the extensions folder: `[Installation root]\oware\synergy\extensions`
2. Restart web portal (Synergy) process.

Synergy Portal Updates (netview.war)

△ CAUTION:
Do this when no users are on the system. Apply this to all web servers.

With the portal running and the tomcat catalina log being tailed:

1. Navigate to `[Installation root]/oware/synergy/tomcat-x.x.xx/webapps` and delete the `netview` directory. After a brief pause you should see it being undeployed in the log.
2. Drop the new `netview.war` into the directory `[Installation root]/oware/synergy/deploy`. Wait a few minutes and you should see it hot deploy the new WAR file and load registry items.
3. After this is deployed, shut down the web servers.

△ CAUTION:
Ensure no old copies of netview.war remain in the [Installation root]/oware/synergy/deploy folder. This software automatically deploys any files in this folder. This will cause a conflict.

Synergy Portal Updates (NetviewFactory.war)

1. Shutdown your system (both webserver/appserver processes).
2. Navigate to `[Installation root]/oware/jboss-x.x/server/oware/deploy`. Apply `NetViewFactory.war` by overwriting any existing version with the new one.

License Installation

1. Stop the application or mediation server.
2. Rename the old license file (`[Installation root]\license.xml`)
3. Copy the new license file to your installation's root.
4. Rename it to `license.xml` if it is named anything else.
5. Open a shell and cd to your installation root.
6. Source the application's environment (Windows: `oware`. Linux `. /etc/.dsienv`)
7. Type `licenseimporter license.xml`

SMTP Mail Sender

If you require a sender / reply to e-mail address on mail sent, you can configure that with the following property (as always, it's best to override in `owareapps/installprops/lib/installed.properties`)

```
redcell.smtp.returnaddress.name
```

14

Localization

OpenManage Network Manager (OMNM) text appears in these distinct entities: menus, forms and fields, and messages. The OMNM Internationalization feature lets you alter the text for each of these entities to the language appropriate for a particular locale. The following sections provide what you need to do this.

Localization Overview – 420
Adding the Language Portlet – 420
Localizing Events – 421
Localizing Events not in Event History – 423
Localizing Resource Bundles – 425
Localizing Message Files – 426
Overriding MIB Text for Event Names – 427
Caching Message/Property Files – 427
Creating Property Files for Double-Byte Characters – 428
Understanding the Message Properties Files – 429
Producing the Properties List – 430
Altering Double-Byte Characters in Audit Trails – 431

Localization Overview

The installation wizard detects the operating system's default language and installs the OpenManage Network Manager (OMNM) software so its default language. If you want the OMNM software installed with English regardless of the installation platform's default, remove the SynergyI8N.jar file from Synergy.zip file before you install.

NOTE:

This should have been done as part of your pre-installation tasks.

The properties settings that force a particular locale for messages are the easiest to change. Only English message files ship with the software. You can override them as needed.

Setting the language property to an empty string in installprops/lib/installed.properties file applies the operating system's defaults.

Override the following Locale properties in that file:

```
oware.resourcebundle.language=en
oware.resourcebundle.country=US
oware.resourcebundle.language.variant=
```

The **language value** must be a valid ISO Language Code. These codes are the lower-case, two-letter codes as defined by ISO-639. Use your preferred search engine to find a full list of these codes at a number of sites.

The **country value** must be a valid ISO Country Code. These codes are the upper-case, two-letter codes as defined by ISO-3166. Use your preferred search engine to find a full list of these codes at a number of sites.

The **variant value** is a vendor or browser-specific code. For example, use WIN for Windows, MAC for Macintosh, and POSIX for POSIX. Where two variants exist, separate them with an underscore, and put the most important one first. For example, a Traditional Spanish collation might construct a locale with parameters for language, country, and variant as: `es, ES, Traditional_WIN`.

CAUTION:

Multilingual support does not necessarily extend to all application add-ons.

Adding the Language Portlet

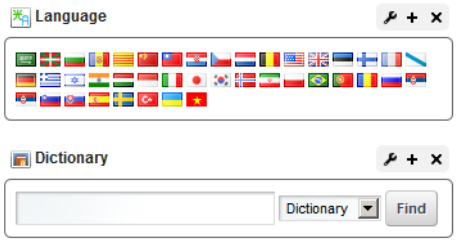
The Language portlet displays flags indicating languages available for many non-OMNM portlets and menus. By default, this portlet does not reside on any OMNM pages.

Add the Language portlet as follows.

1. Select the page on which you want to add this portlet.
2. Select the Add > Applications menu option.

   The application list is displayed.
3. Select Portal Applications > Tools > Language.
4. Click Add.

Note that the Dictionary is a seperate portlet. Follow these similar steps to add the Dictionary portlet.



5 Click a flag to change menus and titles to the related language for non-OMNM portlets and menus.

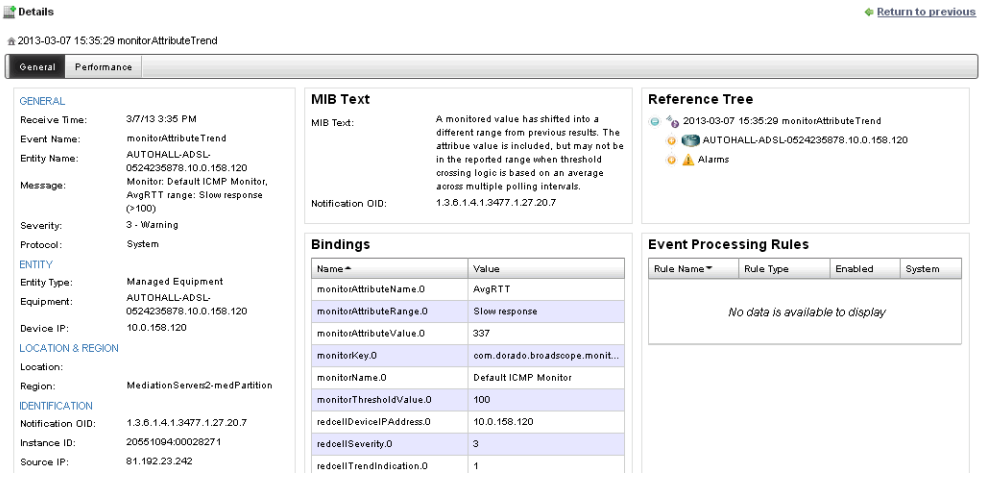


Localizing Events

If your events' MIB is in a language you want translated, the event MIB description is in English. Localize events from the Alarms or Event History portlets as follows.

1 Right-click the event and then select Details.

The Details portlet displays the MIB text.



2 Select the text and copy it to the clipboard.

3 Paste it into your favorite translation site (such as translate.google.com.



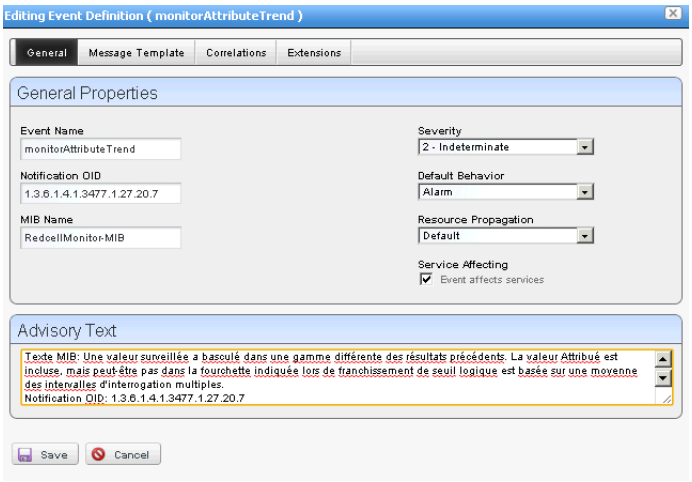
4 Copy the translated text to the clipboard.

5 Return to the portlet used in step 1.

6 Right-click the event and then select Edit > Event Definition.

The Editing Event Definition window is displayed.

7 Paste the translated text into the Advisory Text field.



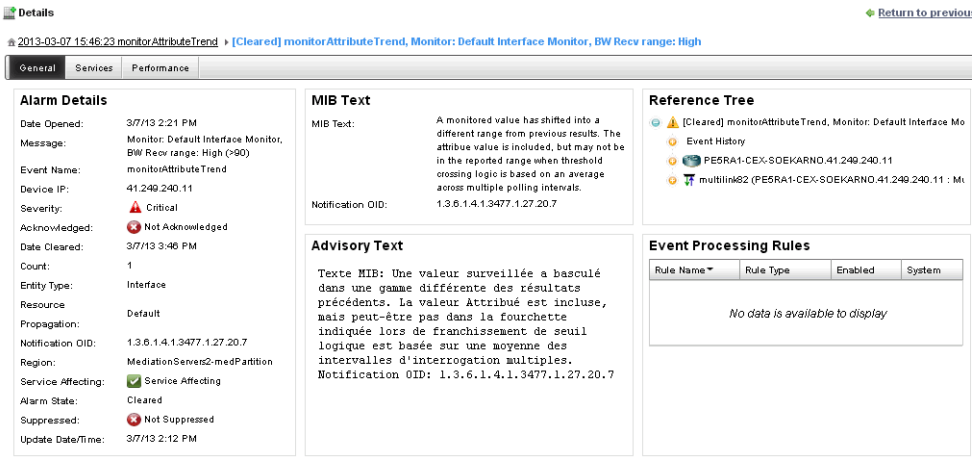
8 Click Save.

9 Right-click the event and then select Details.

The Details portlet displays the advisory test.

NOTE:

Advisory Text only appears in the Details of Alarms, not Events.



Localizing Events not in Event History

Localize events that are not in Event History fas follows.

1. Note the MIB name for the event you want to localize.

   For example, the lldpRemTablesChange event is in LLDP-MIB.

2. Navibate to the Managed Resources portlet.
3. Right-click any resource and then select Direct Access > MIB Browser.

   The MIB Browser window is displayed.

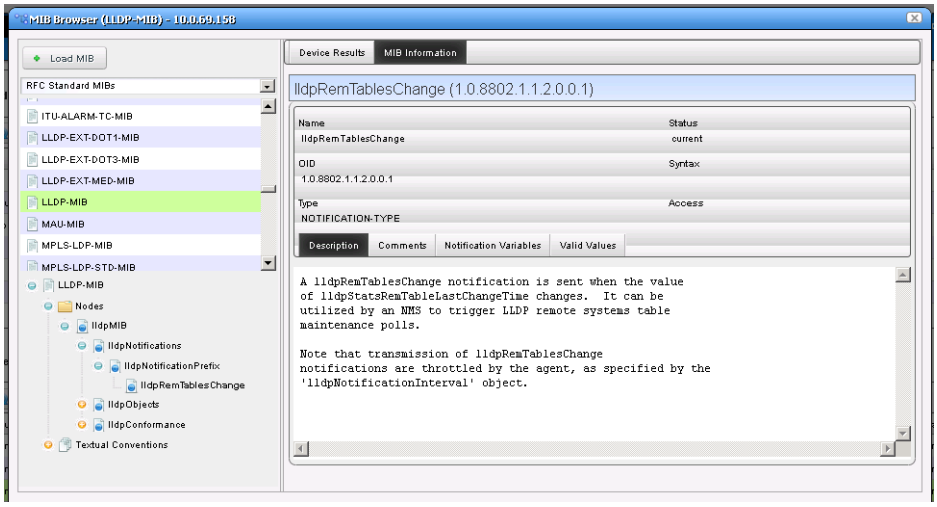
4. Locate the MIB note connected to the event.

   For example, navigate to the lldpRemTablesChange event in LLDP-MIB by expanding:

   `LLDP-MID > lldpMIB > lldpNotifications > lldpNotificationPrefix`

5. Click the MIB Information tab.

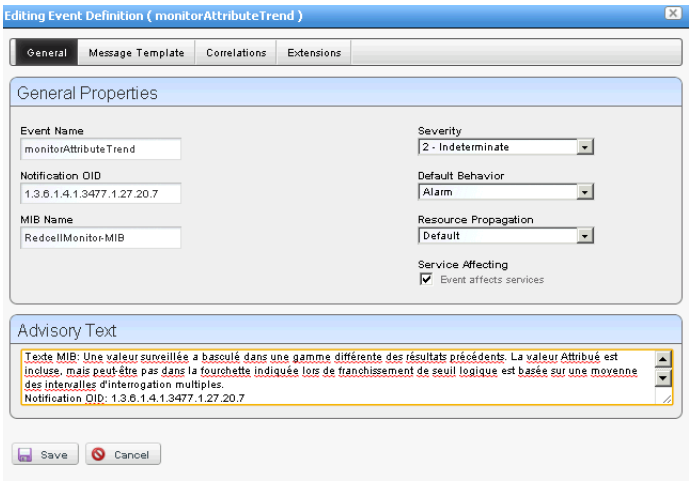
The description text is displayed.



6 Copy the text to the clipboard.

7 Right-click the event and then select Edit > Event Definition.
The Editing Event Definition window is displayed.

8 Paste the translated text into the Advisory Text field.



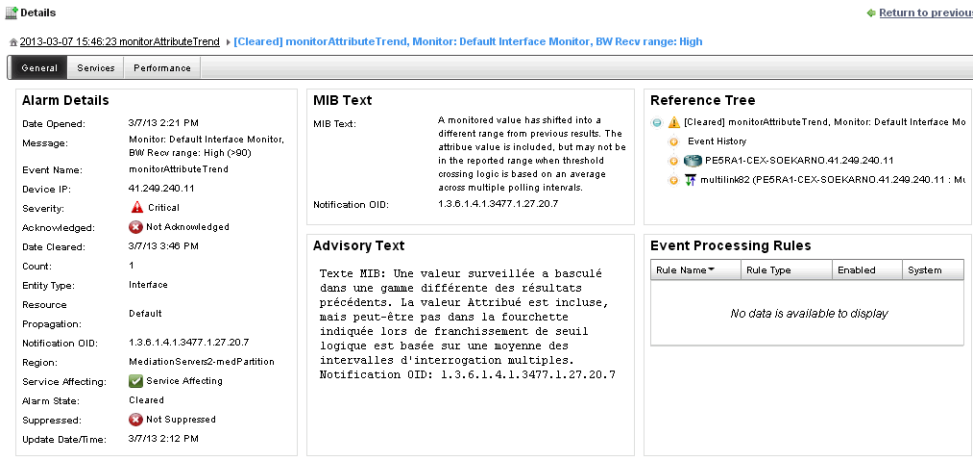
9 Click Save.

10 Right-click the event and then select Details.

The Details portlet displays the advisory test.

NOTE:

Advisory Text only appears in the Details of Alarms, not Events.



Localizing Resource Bundles

You can localize some OpenManage Network Manager (OMNM) text that is not in Localizing Message Files (described below), but in resource bundles. Resource bundles let you localize static labels and button text on forms. These resource bundles are in .jar files, and load automatically based on the locale settings on the operating system where you installed the OMNM software. See Producing the Properties List on page 430 for more about file naming.

Resource bundles exist in msgs.jar files like owareapps\redcell\lib\rcform_msgs.jar. The msgs.jar portion of this filename is common to all existing resource bundles.

The resource bundle for each form contains an ASCII properties file in the same directory as the form class. For example, “form_A” in the “com.driver” package would be named:

```
com/driver/form_A.properties
```

This properties file contains text like:

```
#Resource bundle for Oware form com.driver.form_A
lblName.text=Name
lblName.tooltipt=Enter your name here
```

To localize this resource bundle into “Spanish/Mexican,” the resource bundle for form_A in the com.driver package, is an ASCII properties file in the same directory as the form class, and is named:

```
com.driver.form_A_es_MX.properties
```

With text like:

```
#Resource bundle for Oware form com.driver.form_A
lblName.text=Nombre
lblName.tooltipt= Incorpore su nombre aquí
```

By default, a blank follows the equal sign, and the form displays the text specified when it was created. To override the default, add your text after the equal sign, and create your own .jar with that modified file, named as specified in Producing the Properties List on page 430. Note that not only the .properties files must follow this convention, you must also name the .jar file containing them to reflect the locale.

Localizing Message Files

A message file is a property file. The file name dictates which locales it applies to. The suggested naming convention is as follows:

`<prefix>msgs[_languageCode[_countryCode[_variantCode]]].properties`

Do not provide more precision than necessary. By default, all message files are named as one of the following:

```
<prefix>msgs_en.properties (English)
<prefix>msgs.properties (language independent)
```

No support exists for prepend or append operations.

All entries must follow this syntax: category.number=message text

To find all available message files, search the installation root and all its directories for `*msg*.properties` or `*.msgs` files

Finally, extract the synergy-i18n.jar file into the oware/synergy/extensions directory, edit the appropriate files in the localization subdirectory, then re-compress the .jar file.

△ CAUTION:

If you take the time to translate these files, make sure you keep a copy of any modified files because any upgrade may return them to their original state. You must manually copy the localized files to their original positions to see those translations after any update.

The localization/language functionality comes from Liferay. You may find additional information regarding localization on www.liferay.com/documentation.

Overriding MIB Text for Event Names

You can override default MIB text for event names and descriptions using a text file with the .properties extension in the owareapps/[device driver name]/lib or owareapps/installprops/lib directory to include the override messages. For example:

```
# Below is an example overriding the default redcellDiscoveryJobBegin
   event Name and MIB Text with NEC CX specific information
#
# 1.3.6.1.4.1.3477.1.6.7.3 is the redcellDiscoveryJobBegin Notification
   OID
#
# 1.3.6.1.4.1.3477.1.6.7.3.1=cx2900NMDiscoveryJobBegin
# 1.3.6.1.4.1.3477.1.6.7.3.2=CX2900-NM discovery job begin notification
   indicates a discovery job has been executed
#
1.3.6.1.4.1.3477.1.6.7.3.1=cx2900NMDiscoveryJobBegin
1.3.6.1.4.1.3477.1.6.7.3.2=CX2900-NM discovery job begin notification
   indicates a discovery job has been executed
```

This overrides the redcellDiscoveryJobBegin notification.

With such overrides you can alter event names and notification descriptions. These event names and descriptions are visable in the Event Definitions manager.

To do this, create your own properties file in a text editor (for example, myfilemsgs.properties) and put it either in the driver's lib directory, or in owareapps/installprops/lib directory if you do not want this file overwritten by any application upgrades.

Caching Message/Property Files

The OpenManage Network Manager system loads all message files when it loads properties. The application creates a temporary cache under the oware/temp/msgs directory for the client and the oware/temp/appserver/msgs directory for the server. Subsequent loads use this cache unless a property file or message file was modified (messages are in separate cache).

Creating Property Files for Double-Byte Characters

Properties files must be in escaped unicode format for the properties to appear in a double-byte character set. Create properties files for double-byte character format as follows.

1 Open an editor that is UTF-8 capable.

NOTE:

Notepad UTF-8 files do not work because notepad inserts a Byte Order Mark at the beginning of UTF8 streams.

2 Enter the properties in the text editor using any available double-byte character entry method.

3 Save the file as UTF8 - No Signature.

4 Convert this file to unicode-escaped ANSI format by running the native2ascii Java utility .

You must specify the source and target file in the command. For example:

```
native2ascii -encoding UTF8 chinese-utf8.properties chinese.properties
```

These steps are just an example. Make sure the final file is named appropriately to match the Oware naming standard previously described. This file displays double-byte characters on Windows double-byte versions.

Understanding the Message Properties Files

Following the convention cited in Localizing Message Files on page 426, the name of a Spanish-language (Español) message properties file intended for use in Mexico would be:

`rcmsgs_es_mx.properties`

The entries in this file are grouped according to function. If you want to create a local language version of the OpenManage Network Manager messages, edit the message properties file and translate the message portion of each entry into the language appropriate for your site.

Edit the Message Properties file with any text editor that renders the characters you need. Double-byte characters are allowed, but the OpenManage Network Manager application supports only left-to-right text rendering. The following example shows an an edited message properties file with Italian translations.

```
#
# rcmsgititaliano.properties
# Ciò è l'archvio italiano del messaggio per il nucleo 4.1 di Redcell
#

RC_GENERAL.1=Aggiunta Nuovo
RC_GENERAL.2=Modificando "
RC_GENERAL.3="
RC_GENERAL.4=Prevista Scoperta
RC_GENERAL.5=Modificando
RC_GENERAL.6=Programmazione"
RC_GENERAL.7=Programma
RC_GENERAL.8=Previsto Evento
```

Producing the Properties List

Product a properties list as follows.

1. Shut down the application server.
2. Add the following section to the OMNM log4j.xml file (such as \owareapps\redcell\server\conf\redcell-log4j.xml):

```
<category name="com.dorado.redcell.appframework.nav.RCNavI18NHelper">
  <priority value="TRACE"/>
</category>
```

3. Restart the application server.
4. Open the application server log file once the application is running. T

   The server log is in the \oware\jboss-5.1\server\oware\log\server.log directory.
5. Search for the following properties information in the server log:

```
--- I8N: Redcell Navigation Tree --------------
You should find something that looks like this:
--- I8N: Redcell Navigation Tree --------------
- Place the following list in a message file and replace each value.
- If the property is already in place, the retrieved value is displayed.
RCMenuObject.I18N.menu_reportManager.1=Reports
RCMenuObject.I18N.leaf_templateMgr.1=Report Templates
RCMenuObject.I18N.leaf_reportsMgr.1=Reports
RCMenuObject.I18N.menu_inventory.1=Inventory
RCMenuObject.I18N.leaf_deviceDiscWiz.1=Resource Discovery
RCMenuObject.I18N.leaf_equipMgr.1=Resources
RCMenuObject.I18N.leaf_equipRoleMgr.1=Resource Roles
…
…
…
RCMenuObject.I18N.leaf_RetentionPolicy.1=Retention Policies
--- I8N: Redcell Navigation Tree --------------
```

NOTE:

The above is an example. Menu item order can differ from this example.

Altering Double-Byte Characters in Audit Trails

To see double-byte characters in audit trail messages, you need to alter the database, as described in the following sections.

- Setting Up MySQL
- Setting Up Oracle

Follow the steps outlined for your database type.

Setting Up MySQL

Setting up your MySQL database for double-byte characters in audit trail messages as follows:

1 Stop MySQL using one of the following commands:

- On Windows, execute this as an administrator;

```
net stop mysql
```

- On Linux, execute this as root:

```
/etc/init.d/owaredb stop
```

2 Open the MySQL configuration file in a text editor:

- Windows file is %SYSTEMROOT%/my.ini
- Linux file is /etc/my.cnf

3 Add the following lines to the [mysqld] section:

```
default-character-set=utf8
default-collation=utf8_general_ci
character-set-server=utf8
collation-server=utf8_general_ci
init-connect='SET NAMES utf8'
skip-character-set-client-handshake
```

4 Restart MySql.

- On Windows, execute this as an administrator:

```
net start mysql
```

- On Linux, execute this as root:

```
/etc/init.d/owaredb start
```

5 Run dbevolve.

- On windowb2s execute as the install user:

```
oware dbevolve -x
```

- On Linux,

```
. /etc/.dsienv
dbevolve -x
```

Setting Up Oracle

Set up the Oracle database for double-byte characters in audit trail messages by selecting the UTF8 character set when creating an Oracle database.

```
CREATE DATABASE owbusdb CHARACTER SET UTF8;
```

For existing databases, Oracle has extensive documentation regarding character set selection and conversion. Refer to download.oracle.com/docs/cd/B10501_01/server.920/a96529/ch10.htm.

The simplest form of this is as follows:

ALTER DATABASE owbusdb CHARACTER SET UTF8;

15

Integrating with Other Dell EMC Products and Services

This section provides the following instructions to integrate the Dell EMC OpenManage Network Manager application with other Dell EMC products and services:

Synchronizing with OpenManage Essentials – 434

Activating Dell EMC SupportAssist – 435

Generating System Performance Summary – 438

Configuring Dell EMC Warranty Reporting – 439

Synchronizing with OpenManage Essentials

The OpenManage Essentials (OME) product is a separate product from the OpenManage Network Manager (OMNM) product. The OME product is also used for some system management operations. However, it has fewer overall features than the OpenManage Network Manager product. If you are already using the OME product to manage computer systems such as servers, it is possible to configure the OpenManage Network Manager product so that all of your OME data is available through the OpenManage Network Manager application.

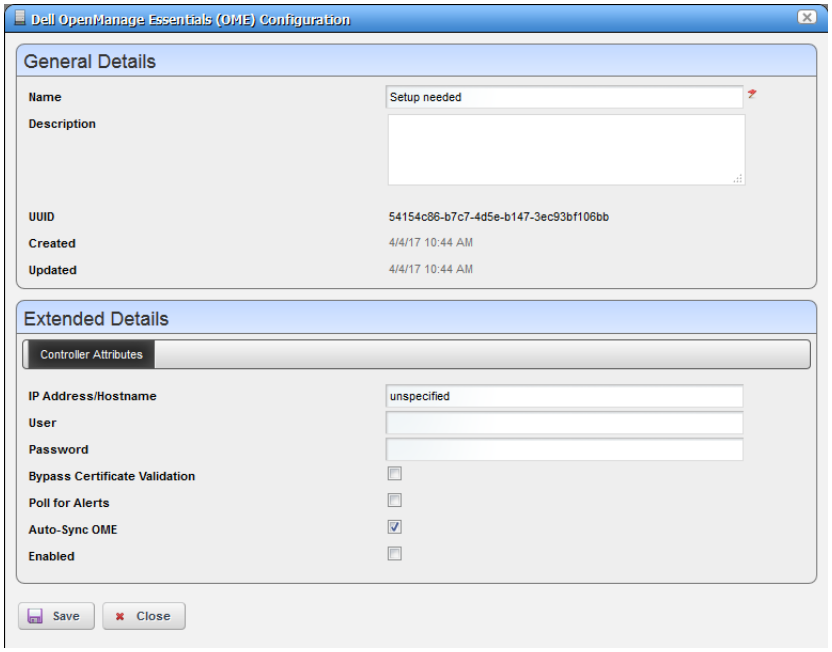
Synchronize the OME product with the OpenManage Network Manager product as follows.

1 Navigate to the Setup Tasks portlet.

2 Find the OpenManage Essentials (OME) Configuration entry.

3 Select the Edit action.

The Dell EMC OpenManage Essentials (OME) Configuration window is displayed. The default configuration name is *Setup needed*. You can change the name to reflect the OME server name.



4 Optionally enable OME.

a. Select Enabled.

b. Enter the OME server IP address or hostname.

c. Enter your OME login user name and password.

5 Select the following optional configurations as needed:

- **DBypass Certificate Validation** when selected, the default security verification is disabled allowing communication with servers that use self-signed, expired, or otherwise invalid security certificates.
- **Poll for Alerts** when selected along with the Enabled option, the OpenManage Network Manager application regularly polls the OME application for alerts so that any alerts that

are created within the OME application will become events and possibly alarms within the OpenManage Network Manager system.

Common OME alerts include omeAlertSystemUp and omeAlertSystemDown. It is possible to configure the OME application to forward alerts to the OpenManage Network Manager application, which would eliminate the need to poll for such alerts. If you configured the OME application with a rule to forward alerts to the OpenManage Network Manager application, then it is recommended that you **do not** select this option.

- **Auto-Sync OME** when selected along with the Enabled option, the OpenManage Network Manager application automatically synchronizes to all devices that the OME application has under management.

  When you save this configuration, the OpenManage Network Manager application communicates with the OME application and creates managed resources corresponding to every device in the OME inventory. The save also creates a recurring schedule item is that periodically synchronizes the OME application with the OpenManage Network Manager application.

- **Enabled** when selected, the OpenManage Network Manager application communicates with the OME application.

  If not selected, the OpenManage Network Manager application **does not** sync to the OME application or poll for OME alerts. At any time, you can change the OME configuration from enabled to disabled or vice-versa.

6 Save the configurations.

7 Verify that OME managed devices now show in the Managed Resources portlet.

NOTE:

In most cases, the OME data shown in the Managed Resources portlet is the same as what shows in OME product but there are some exceptions. For example, the OME application states that a device type is Unclassified but the OMNM application considers the equipment type to be Server.

Activating Dell EMC SupportAssist

The Dell EMC SupportAssist feature provides automated, proactive and predictive technology that reduces troubleshooting steps and speeds up your resolution time. The SupportAssist feature collects information from supported devices and automatically creates support cases when issues arise. This helps Dell EMC to provide you an enhanced, personalized, and efficient support experience. The default setting for this feature is Opt-Out but you can select Opt-In.

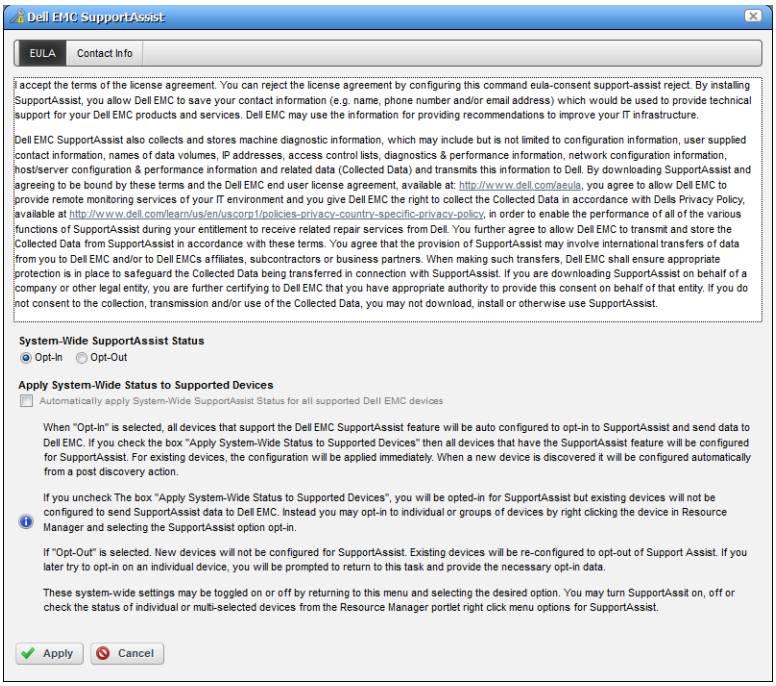
Activate the Dell EMC SupportAssist feature as follows.

1 Navigate to the Setup Tasks portlet.

2 Find the Dell EMC SupportAssist entry.

3 Select the Edit action.

The Dell EMC SupportAssist window shows the End User License Agreement (EULA) panel.



4 Select the appropriate System-Wide SupportAssist Status option (Opt-In or Opt-Out).

Note that this controls whether or not the OpenManage Network Manager application is synced with the SupportAssist feature at the system-wide level and this status is not necessarily applied at the device level.

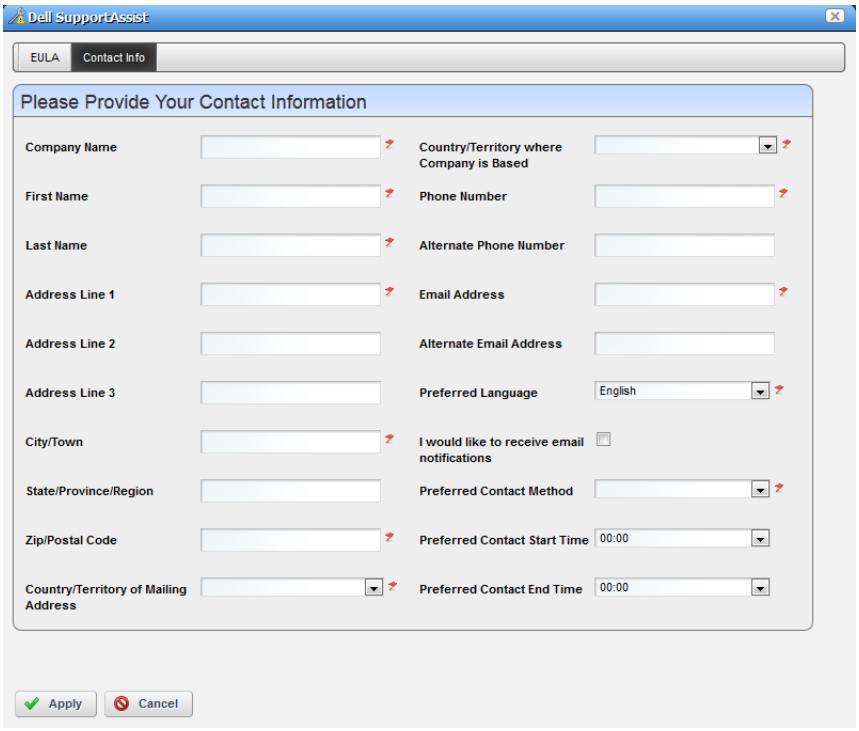
5 Optionally select Apply System-Wide Status to Supported Devices. Otherwise, continue with step 6.

If selected, the system-wide status automatically applies to all supported devices under management and all newly discovered devices that support this feature. If **not selected**, the status **does not** automatically apply to any devices.

6 Click Apply if you selected the Opt-Out option in step 4. Otherwise, continue with step 7.

7 Click the Contact Info tab if you selected the Opt-In option in step 4.

The Contact options are displayed.



8 Enter the required fields.

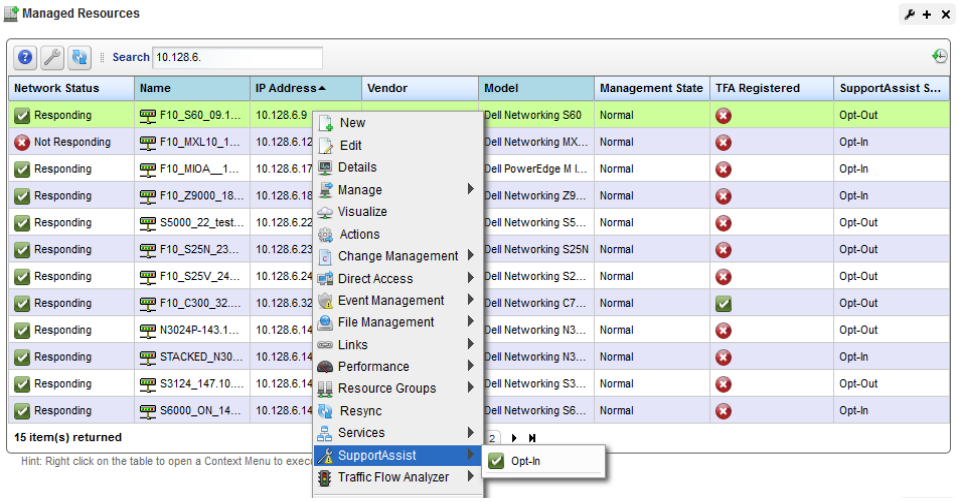
Dell EMC SupportAssist needs this information to provide your company or organization with support to help optimize the OpenManage Network Manager application and any Dell EMC equipment under management.

9 Click Apply.

After you apply the System-Wide SupportAssist settings, you can still change the SupportAssist status for any device in inventory, if the System-Wide SupportAssist Status is set to Opt-In. If the System-Wide Status is Opt-Out, all devices remain as Opt-Out.

If you have selected Opt-In at the system-wide level, the SupportAssist > Opt-In/Out pop-up menu option is available from the OMNM Resources > Managed Resources portlet for **only** Dell EMC devices. Right-click any Dell EMC managed equipment listed in the Managed

Resources portlet to change the SupportAssist status to Opt-In or Opt-Out depending on its current status.



If any given device's SupportAssist status is set to Opt-In, that device sends usage data to Dell EMC products. However, the OpenManage Network Manager server **does not** automatically send any system-wide usage data to Dell EMC products. If you want to send data to Dell EMC from the OpenManage Network Manager application to help optimize your system, generate a system performance summary and send it to the Dell EMC optimize team.

Generating System Performance Summary

The OpenManage Network Manager server **does not** automatically send any system-wide usage data to Dell EMC. If you want Dell EMC to help optimize your system, generate a system performance summary file and then send it to the Dell EMC optimize team. The Dell EMC optimize team reviews the data and offers advice on how to optimize the performance of your system.

Generate a system performance summary file as follows.

1. Navigate to the Resources > Actions page.
2. Search the Actions portlet for "Generate system performance summary file."
3. Right-click on it and then select Execute.

   The Executing Action is displayed.
4. Execute this action now or else you can schedule this action to execute on a regular basis, such as once a day.

   A system performance summary file is created and placed in the application server file system. The Job Viewer panel displays the file location.
5. Transfer the file to the Dell EMC optimize team using FTP (or some other agreed upon transfer method).

   If you configured a schedule to generate this file on a regular basis, you can set up a process that automatically transfers these files to the Dell EMC optimize team when they are generated.

Configuring Dell EMC Warranty Reporting

Dell EMC manufactured devices might have warranty information associated with them. You can configure the OpenManage Network Manager (OMNM) application to synchronize with the warranty information in the Dell EMC database for each Dell EMC device that is under management. If warranty information is in the OMNM database, you can view and report on this information and receive alarms when any warranty is nearing expiration or has expired.

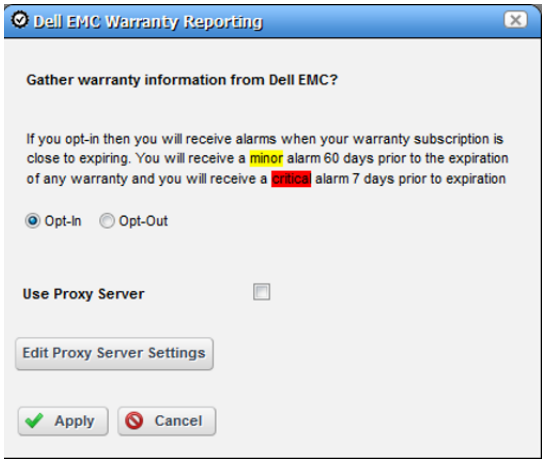
Configure a Dell EMC warranty report as follows.

1 Navigate to the OMNM the Common Setup Tasks portlet.

2 Find the Dell EMC Warranty Reporting entry.

3 Select the Edit action.

The OMNM Warranty Reporting window is displayed.



4 Select whether to Opt-In or Opt-Out.

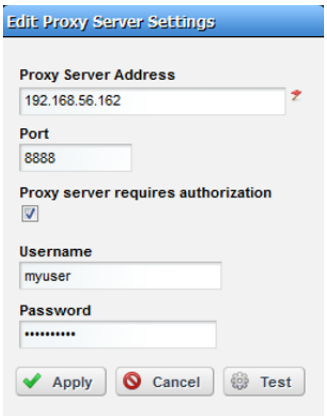
The default is to Opt-In, which means that the OMNM application automatically gathers warranty information from Dell EMC devices. You can generate reports with this information and the OMNM application creates alarms to inform you when the warranty is close to expiration or has already expired.

5 Select the Use Proxy Server option if the OMNM application connects to the internet through a proxy server. Otherwise, skip to step 7.

6 Edit the proxy server settings.

a. Click the Edit Proxy Server Settings button.

The Edit Proxy Server Settings window is displayed.



b. Enter the Proxy Server Address and Port.

c. Select the "Proxy server requires authorization" option if authentication is required to access the proxy server.

d. Enter the Username and Password.

e. Test the connection to the proxy server.

f. Click Apply.

You are returned to the Dell EMC Warranty Reporting window.

7 Click Apply.

The settings are saved.

If you selected Opt-Out, no device warranty information is shared with the OMNM application. If you selected Opt-In, the OMNM application automatically synchronizes with the warranty information in the Dell EMC database for each Dell EMC device that is currently under management and warranty information is saved to the OMNM database. Synchronization also happens whenever a Dell EMC device is newly discovered and brought under management by the OMNM application.

8 Test your warranty configuration.

a. Navigate the Managed Resources portlet.

b. Right-click a Dell EMC device and then select Details.

The devices details are displayed.

c. Click the Maintenance Info tab.

The Maintenance Logs and License and Warranty Info lists should show information relating to the products and services that are licensed and the warranty information relating to the selected device.

d. Run a report of all devices' warranty information from the Reports portlet by searching for Equipment Warranty Status, right-clicking the report, and then selecting Execute Report.

A

OpenManage Network Manager User Interface

This section describes the OpenManage Network Manager user interface pages, portlets, and options that are installed by default. You have the option to add more pages, move the pages on which the portlets appear, or define the portlets to be on multiple pages.

You may not have access to all of these in your installation, or you may not be able to use them with the user permissions you have been assigned by the portal administrator. To see all available OpenManage Network Manager portlets (and a few not connected to OpenManage Network Manager), select Add > Applications. See Applications Available for Use on page 662 for a description of the portlets (applications) that are not accessible from a page by default.

Portal Overview – 442
Home Page – 454
Alarms Page – 473
Network Management Page – 516
Performance Page – 535
Resources Page – 538
Configuration Management Page – 562
Reports Page – 612
Settings Page – 624
Applications Available for Use – 662
Schedule – 671

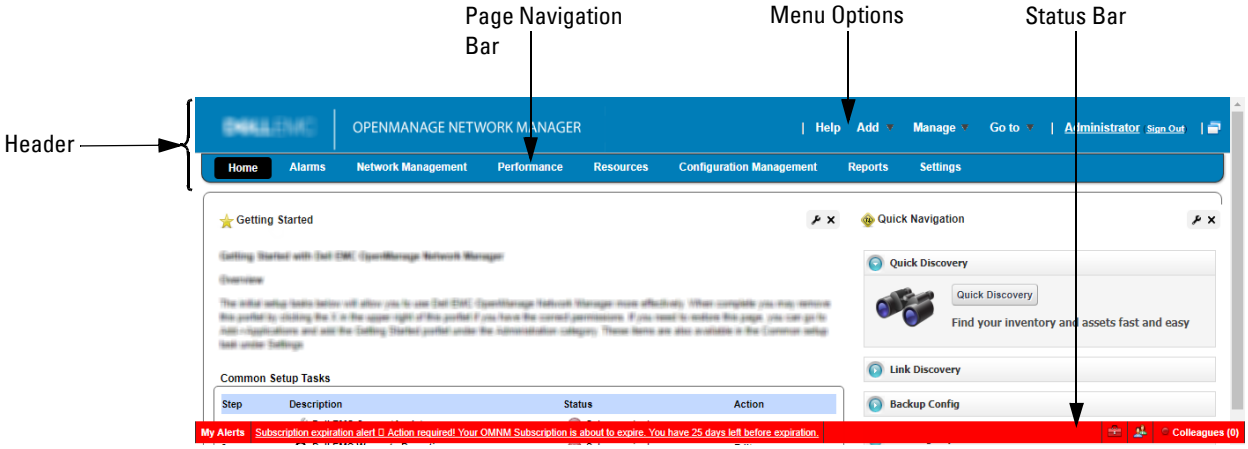
Portal Overview

This section describes the OpenManage Network Manager (OMNM) portal window, general information, and features that are common for multiple portlets.

The **portal header** has the company logo, product name, and its menu options. The *userName* is an active link to the Manage My Account options, where you can configure your name, job title, image, email and so on. You can access these same options from the Go to > Control Panel menu option. The header also includes:

- Sign Out, which logs you out of the OpenManage Network Manager portal. When you sign in, Password Reminder portlet is displayed if your administrator has set this option.
- Full Page Toggle, which expands the window full page or returns to a manually adjustable window.
- The page navigation bar, which provides access to the pages, subpages, and portlets.

The status bar opens My Alert/Action History window, displays subscription expiration alert, access to settings, conferencing, and a list of colleagues on the system.



Menu Options

The following menu options are available from the OMNM portal header.

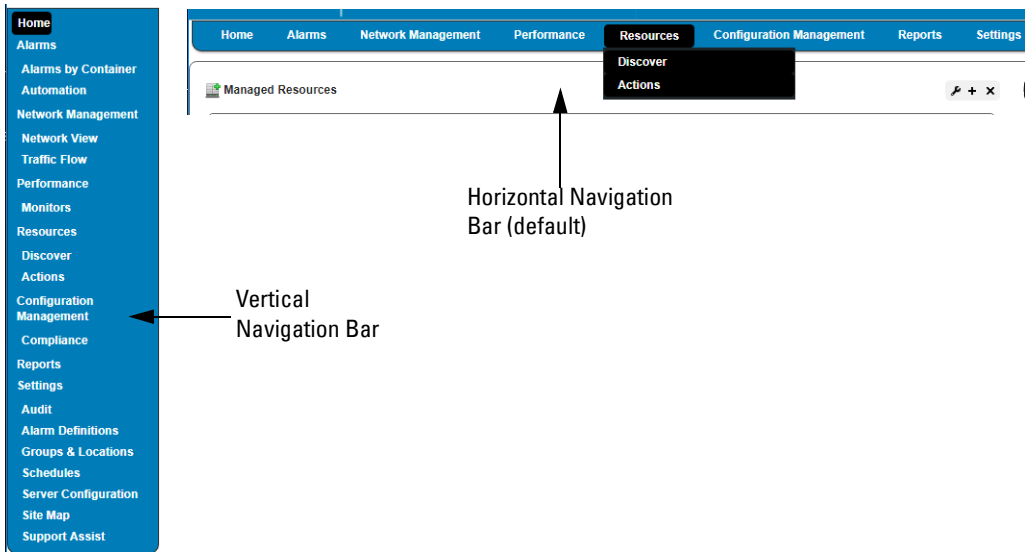
Menu	Description
Help	Opens the OMNM online help.
Add	Lets you create Pages or add Applications (portlets) to an existing page. Select Add > Page and a field opens on the navigation bar when you enter the page name and then click the checkmark. Select Add > Applications and a list of available applications (portlets) is displayed. Navigate to the portlet, click Add, and the portlet is added to the currently selected page. See General Information on page 447 for more information about pages, child pages, portlets, editors, and the applications list.

Menu	Description
Manage	Opens the Manage Page window where you alter the page organization or its layout when you select the Page or Page Layout options. From the Manage Page window, you can drag and drop page locations in the tree, and add child pages. See Creating and Rearranging Pages on page 49 for instructions. The Show Versions option displays information about your current OMNM installation, such as product details, installed extensions, and driver information. This option is not available from the message board portlet.
Go to	Provides access to the Control Panel on page 673 and any other pages (public/private) defined by you or your system administrator. When you add a new community, its configured pages appear in this menu too. Creating public pages requires administrative rights. However, users that do not have administrative rights can only configure their private pages. Changes to a page persist after you make them, provided you have the rights to make changes to that page. See Public/Private Page Behavior on page 676 for the details. Best practice is to use multiple pages within the OMNM system rather than multiple tabs. I you have the Multitenancy (MSP) option installed, these options are not available and MSP offers a different security model.

Page Navigation Bar

Page Navigation Bar

The page navigation bar provides access to the pages and child pages installed by default or the pages and child pages you configured from the Manage > Page menu option. The page navigation bar appears horizontally below the portal header by default, or vertically on the left of the screen. The pages that appear on this bar vary depending on which OpenManage Network Manager package you installed.



If you narrow your browser window, the navigation bar collapses to the left. If you want the virtical navigation bar as the default, change the regular browsers menu position settings to vertical from the Manage Page window.

Status Bar

The status bar is at the bottom of the OpenManage Network Manager (OMNM) portal window. It contains the following elements:

- My Alerts
- Subscription Notification
- Settings
- Conferencing
- Colleagues

My Alerts

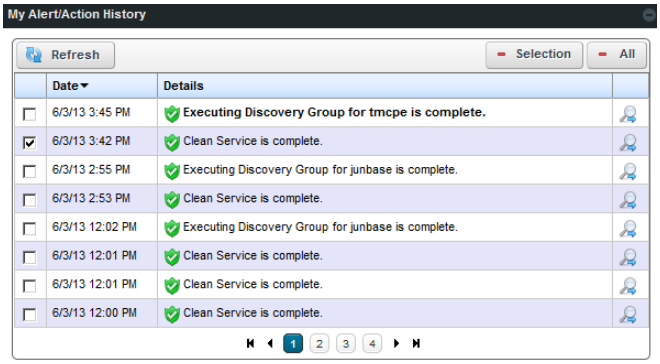
My Alerts opens the MyAlert/Action History window when you click on it. The MyAlert/Action History window displays cataloged messages and notifications you received, including generated reports. From this window, you can:

- Delete selected messages or notificaitons by selecting those you want to delete and then clicking Selection.
- Delete all messages and notifications by clicking All.
- View additional information about the message or notification by clicking the magnifying glass.

You can see the portal when the Web server is up, but the application server is not. When the application server starts after the Web server, an alert appears in the MyAlert/Action History list announcing that application server is up.

CAUTION:

If My Alerts is not receiving messages or notifications, make sure that your firewall is not blocking ports the application uses. See Ports Used on page 697 for a list of ports and more about configuring Linux firewalls.



Subscription Notification

The subscription notification is a warning that your license is nearing expiration. The status bar color changes and displays the following message:

```
Subscription expiration alert: Action required! Your OMNM Subscription is
    about to expire. You have 28 days left before expiration
```

Click the message and the License Viewer, Subscription Information panel opens, where you can start the license renewal process. It also displays the number of days until license expiration.

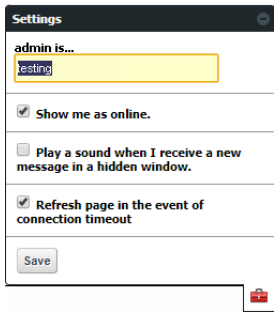
The alarm color reflects the threshold for the number of days remaining before license expiration:

- 60 days or less: yellow status bar
- 30 or less days: red status bar
- 61 or more days status bar does not change colors

Settings

The Settings tool in the status bar lets you configure your user settings for any online chat with your colleagues, including the saying, whether your online presence appears, and whether to play a sound when messages arrive.

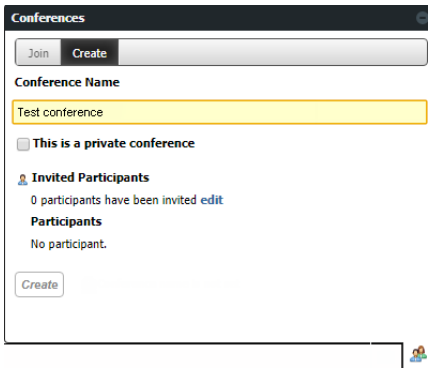
When you have a message from another user, that user's name appears on the status bar to the left of the settings tool.



Conferencing

The Conferencing tool in the status bar lets you share whatever is of concern with other OpenManage Network Manager (OMNM) users and collaborate with more than one person. For example, if a discovered device has problems, you can create a link to the device's from the Connected Devices Portlet and share it with other users with the OMNM internal instant messaging/chat system (see Sharing a Resource on page 87).

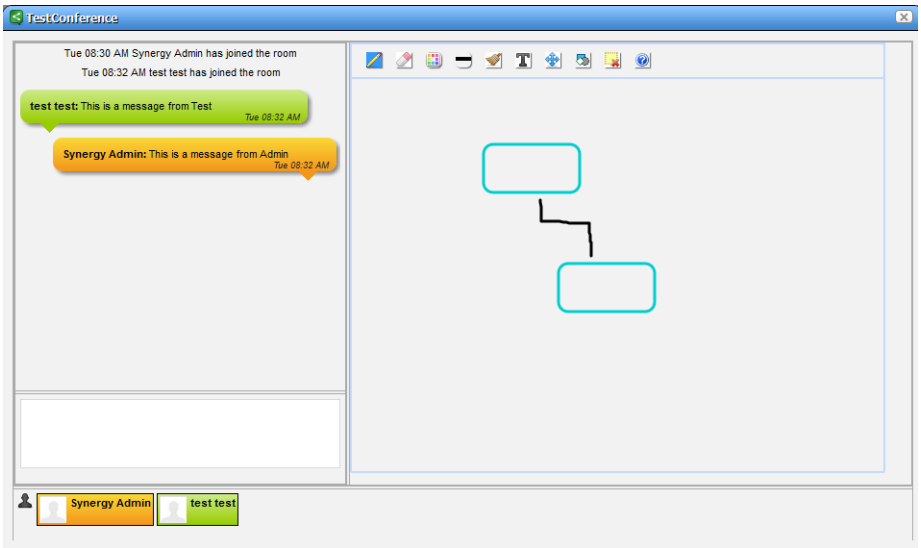
Use the Conferencing tool to configure your user settings for any online chat with multiple colleagues.



The Join options become active when you are invited to a conference. An online chat window appears after you join.

The Create options let you name the conference, specify whether the conference is private (for invites only), and then invite colleagues and configure an invitation message by clicking edit.

Conferencing also opens a screen that both records text and provides a virtual white board where participants can draw.



Hover the cursor over the white board tools at the top to see what they do. Enter text in the lower left corner, and it appears on the left after you click Enter. Conference participants appear with icons and colors keyed to their text in the lowest portion of the screen.

NOTE:

If appearance or performance concerns impede your conferencing, clear your browser's cache, then try conferencing again.

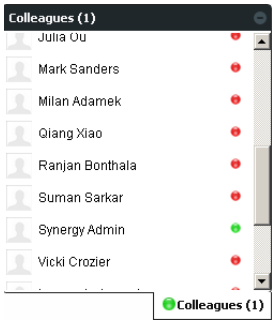
Colleagues

The Colleagues tool has a red dot when you are online alone and a green dot when other users are online. It also shows the number of colleagues online. Click the Colleagues tool and a list of OMNM users is displayed. The title bar shows the number of users online. A green dot indicates the users that are online and a red dot indicates the users that are not online. Click on a colleague and enter text in the popup that appears to send messages. Previous chat history also shows above any current text in the chat popup.

Click the upper right corner (-) to close the window.

NOTE:

You can turn off chat for the application with special branding available through your sales representative, but not for a single user. Chats are stored in the OpenManage Network Manager database, but as blobs, so reading chat history, except the date of chats, is problematic.



General Information

Portlets are the elements of any page within the OpenManage Network Manager (OMNM) portal. Whether you have access to a portlet and from which page a portlet is accessed is defined by your system administrator. In your environment, a portlet could be accessed from multiple pages. See the description of each portlet for more details.

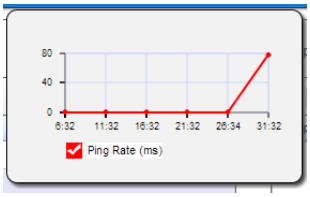
Here are some common portal features related to portlets:

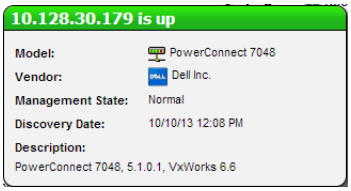
- **Customizable** pages by dragging portlets to a different location, adding portlets, or deleting portlets. The applications list shows all the available portlets when you select the Add > Applications menu option.
- Viewing data from both a summary view and an expanded portlet view for most portlets.
- **Sorting** on a column by clicking on that column's heading. Reverse the sort order by clicking it again. This only sorts what appears in the portlet, whether expanded or not. The application remembers each user's choice saving the last Sort Column and Order on any page. The arrow to the right of that heading's text displays the sort direction (ascending or descending). When the arrow appears in a heading, the selected column is the basis for sorting.
- **Resizable** columns by dragging the header border.
- **Print** a portlet's content by exporting by exporting its expanded view content to a PDF, Excel, or CSV file, open the exported file in the appropriate application, and then printing it.
- All **time stamps** are based on the users timezone. It is based upon Greenwich Mean Time (GMT) and changes depending upon the timezone that you are in when viewing a record.

- Some portlets include editors that appear after you select an item, right-click, and then select either New or Edit.

  Mandatory fields in these editors appear with a red flag icon to their right. That flag may disappear once you fill in the field. Mandatory fields in an Action appear with a red flag icon to their right. That flag disappears once you add the action to an Action Group.

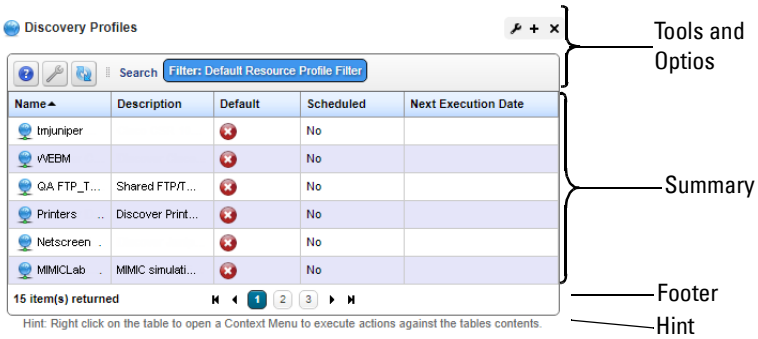
- Standard **tooltips** show for most portlet field's content, which is useful when the field cannot show all its content. Windows and editors have help tooltips when you click the question mark next to a field.or what goes into a field in an editor when you hover over the cell/field. For cells where a question mark appears when you hovering over a listed item, a more detailed tooltip is displayed or a graph (in the Top N portlets) is displayed.





If a graph is displayed, it can line, bar or pie graph, depending on the portlet, device and activity monitored. The more detailed tooltips require the latest Adobe Flash for full functionality.

This section describes common portlet features, such as the portlet tools and options, summary, footer, and hint.



Portlet Tools and Options

The following portlet tools and options apply to all OMNM portlets, where available. Specific portlet features and functions are described in their respective section.

Tool	Description
	Provides access to the following options: **Look and Feel**, where you configure the portlet text styles, background, border, margin and padding, advanced, and WAP styles. **Configuration**, where you specify whether users have view, add to page, configuration, and permissions based on their assigned role. You can also specify whether to share the portlet with a website, Facebook, OpenSocial gadget, Netvibes, or Friends.
+	Displays a expanded portlet and provides additional information and options. Click Return to previous to return to the initial portlet view. This tool shows only for those portlets that have the Maximize option.

Tool	Description
X	Removes the portlet from the existing page.
Return to previous	Takes you back to the previous page (initial portlet). Some examples where this option shows are the expanded portlet and details portlets. Although browsers have a back button, the Return to previous option is the most dependable wat to reture to a previous page, window, portlet, and so on within the OMNM portal.
	Displays online help for the selected portlet. Once you access the online help, you also have the option to search the help for other topics.
	Opens a Settings window, where you filter the results and specify which columns to include and their settings. In some portlets, such as Alarms, this option can configure whether charts or graphs appear. See Modifying Column Settings on page 85 for instructions. Column selections from the portlet are not propagated to the maximized view. If you want the same columns for both views, you must select them for each view.
	Isolates the browser's page refresh to the selected portlet so that you do not have to load the entire window again. After you modify a portlet's settings, click the refresh tool to see your changes.
Search	Filters the list to show more specific items. Select from the list of user-defined filters. This searches all available items in the database, whether they appear listed or not.
	Displays the first page in the list.
	Displays the previous page in the list.
	Displays the next page in the list.
	Displays the last page in the list.

Summary

The portlet summary supports displaying up to 200 rows, the expanded portlet supports up to 1000 rows. Using the portlet filtering capability makes more sense than trying to see more rows. (See Defining Advanced Filters on page 86 for instructions.)

To act on listed items, right-click the item and then make a selection from the popup menu. The menu options available depend on the portlet and the row selected.

To see information about listed items in a portlet, hover over the row until a arge tooltip displays more details.

Footer

The footer lists the number of items returned, the limit reached in red if you specified a maximum for the list, and the navigation buttons. The navigation buttons are the standard go to first/last page, move back/forward one page at a time, and select the page to go to.

Hint

The hint at the bottom of the portlet lets the user know that right-clicking the table opens a popup menu (context menu) listing the available actions. By default, this hint is there for every portlet. If you **do not** want the hint showing, set the show.portal.hints attribute to false in the server-overrides.properties file. See Hiding Portlet Hint Text on page 85 for detailed instructions.

Expanded Portlet

The expanded portlet lets you display more information, do quick searches, do more advanced filters, or export the list to a PDF document or Excel or CSV formats. You can also see details about a selected row in the Widgets panel. Access the expanded portlet from the summary portlet's title bar by clicking the expand (+) tool. Return to the summary portlet by clicking Return to previous.

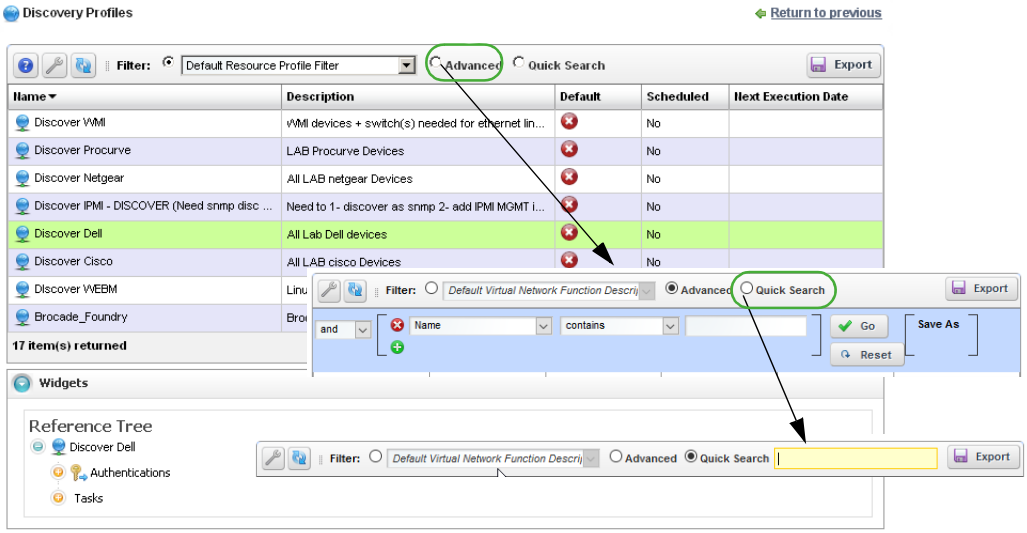
You can perform all the same actions from the expanded portlet and you can from the summary portlet and navigating the list is the same as the summary portlet.

User permissions may limit access to the expanded portlets. For example, the OpenManage Network Manager can have many communities and limit users' memberships. Such users can lightly browse other Communities' screens without full privileges.

See Control Panel on page 673 for more about setting up user privileges for portlets.

NOTE:

Note that Screen size limitations may require you to expand the browser to see expanded screens correctly. You must have at least 1250 pixels in width.



In addition to the options the summary view provides, the expanded portlet provides the following options.

Option	Description
Return to previous	Takes you back to the previous page (initial portlet).
Filter	Displays the default filter and any user-defined filters available. Select a filter from the list. Otherwise, select the Advanced or Quick Search option.

Option	Description
Advanced	Provides options to create conditional (AND, OR) filter statements. Once you create a conditional statement, click GO to view the results. Click Save As to save the filter. Click Reset to create another conditional filter. Otherwise, use the Filter or Quick Search option.
Quick Search	Activates a field, where you type a phrase and then press ENTER. Otherwise, use the Advanced or Filter option.
Export	Saves the current table to PDF, Excel, or CSV format. Click Export, select the format type, and then click Generate Export.
Widgets	Displays one or more detail widgets, such as the Reference Tree. You have the option to show or hide the widget details from the title bar. The Reference Tree also expands/collapses tree elements.

Settings Window

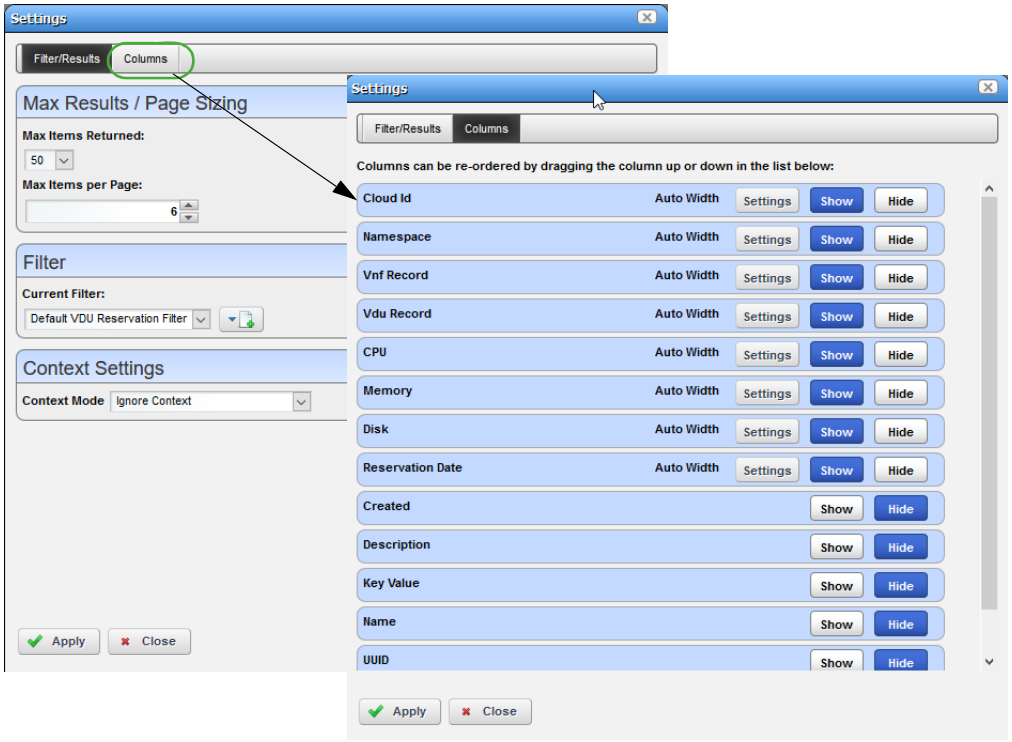
Use the Settings window to set the return results parameters, define a filter, and select the context mode. You can also specify which columns the portlet shows and the settings for each column.

The Filter/Results panel is displayed by default. Click the Columns tab to display the Columns panel.

NOTE:

Column selections from the portlet are not propagated to the maximized view. If you want the same columns for both views, you must select them for each view.

Click the portlets Settings tool to access this window.



The Settings window provides the following fields and options.

Field/Option	Description
Max Items Returned	Sets the maximum number of items the filter returns. Valid values are 2, 25, 50, 75, 100, 200, 300, or 500. For performance reasons, this default value is often relatively low.
Max Items per Page	Sets the maximum number of items displayed per page. Valid values are 4 to 100. For performance reasons, this default value is often relatively low.
Current Filter	Provides a list of user-defined filters from which to choose. The product ships with a default filter. Depending on your permissions, you have the option to create a filter or copy the currently selected filter from which you create a filter. *The* expanded portlet does not include this option. See Defining Advanced Filters on page 86 for alternatives. **Note:** An administrator configures a portlet's default display filter and then clicks the portlet name and renames it. For example, make the default filter in the Managed Resources portlet to display only Dell Routers, then click the Managed Resources portlet name to rename it to *Dell Routers*. If you are not an administrator, you must make a personal page for such portlets if you want the filter settings to persist (not applicable in multitenant environments).
Context Mode	Specifies which of the following context modes the selected portlet uses: • Listen for Context • Ignore Context (default) • Broadcast Context • Broadcast and Listen for Context • Not all portlets have all option.
Columns	Displays a list of columns, their settings, and whether a column is hidden. Select the Column tab to display the columns. The default columns displayed and the available columns vary with each portlet. If you have many instances of a portlet in your environment, the changes made to the portlet or maximized portlet are not global, they apply only to the current portlet or its maximized portlet. Click the Settings button to specify whether the width is automatically set (Auto Width) or specify a specific pixel width. Auto Width is the default. The grayed out Show/Hide button indicates the selection for the column.

Applications List

The applications list is displayed when you select the Add > Applications menu option. When you The application (portlet) list shows some portlets with a purple icon and others with green icons.



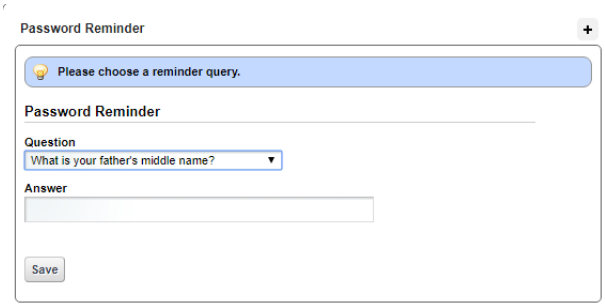
The **purple icon** indicates that you can add **only** one instance to a community and it displays the same data, even if it appears on more that one page, such as the Container View portlet. These are referred to as non-instanceable portlets. Once you a non-instanceable portlet to a page, its entry in the applications list is disabled (grayed out).

The **green icon** indicates that you can add the portlet to many pages with each instance displaying different information, such as the Authentication or Container Manager portlets. These are referred to as instanceable portlets.

Password Reminder

Use the Password Reminder portlet to add another level of security. If set by your administrator, this portlet displays when you sign in to the OpenManage Network Manager portal.

You have the option to pick a question from the list or create your own question.



Home Page

The Home page displays the following portlets by default:

- Getting Started Portlet
- Alarms Portlet
- Managed Resources
- Quick Navigation Portlet
- Search by IP or Mac Address Portlet

Getting Started Portlet

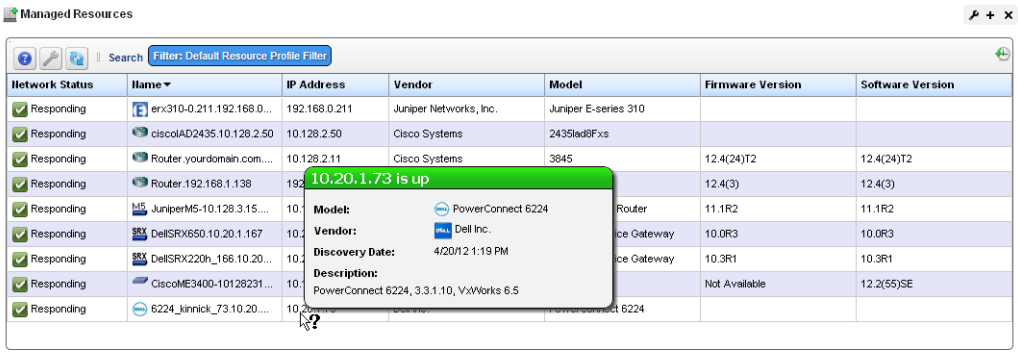
Alarms Portlet

(also located on the Alarms page and the Alarms > Alarms by Container page) By default, this view shows the pie graph and the color legend.

Managed Resources

The *Managed Resources* summary portlet displays the discovered devices on your network, their *Network Status*, *Name*, *IP Address*, *Vendor*, *Model*, *Firmware* and *Software Version*.

(also located on the Resources and Configuration Management page)



Hovering the cursor over a listed device's IP address produces a popup with its alarm status in the headline and additional device information. See the Managed Resources Expanded section for a description of columns and additional capabilities in that version of the portlet. Icons that appear next to the equipment name have some significance. For example:

Icon	Device Type
	Switch
	Router or Switch/ Router

Icon	Device Type
	Wireless Virtual Controller
	Wireless Access Point

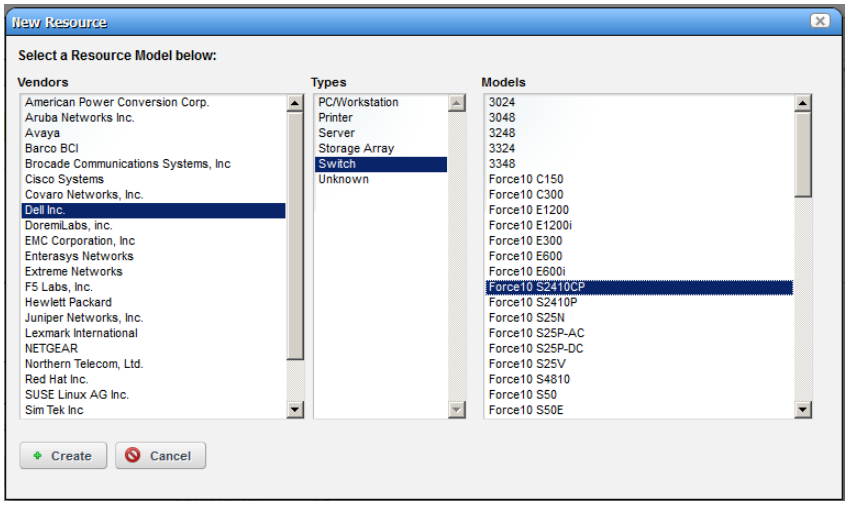
You can schedule actions selected here in addition to executing them immediately. See Scheduling Actions on page 307 for more. Right-clicking a listed resource can display the following menu items:

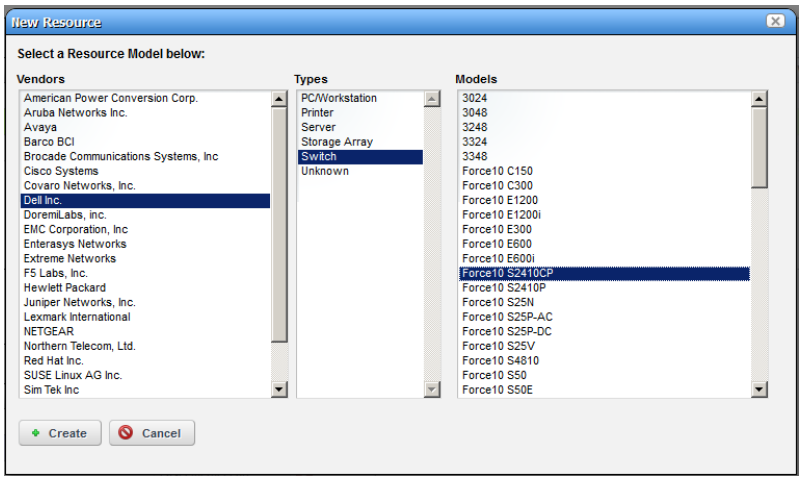
See General > Entity Change Settings on page 687 for the way to set the summary portlet refresh interval. The default is 40 seconds. If this portlet is on the same page as the Container View portlet, or if it is in expanded mode, refresh does not occur automatically, but you can manually refresh it.

NOTE:

A small clock icon in the upper right corner of the portlet indicates that auto refresh is enabled.

New—You can create a new device without discovering it with this menu item. Select the device vendor, model and type in the next screen, then fill in the information about the device in the editor that appears after that selection.





The editor description appears below.

Edit—This lets you use the following screens:

- Resource Editor: General
- Resource Editor: Authentication
- Resource Editor: Management Interface
- Resource Editor: Custom Attributes—This tab appears only if you have configured custom attributes. See Redcell > Data Configuration on page 682 for more about them.

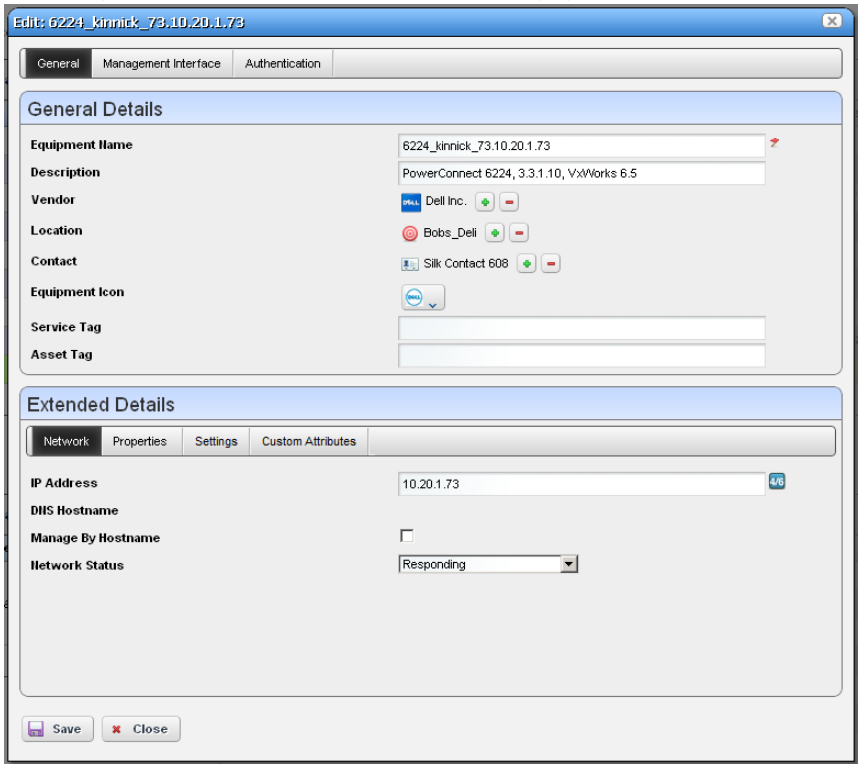
Click *Save* to preserve any changes made in these screens to OpenManage Network Manager's database, or *Close* to abandon any changes made in editor screens. Unless the device is a printer, changes to these screens typically make database changes, not changes on the device.

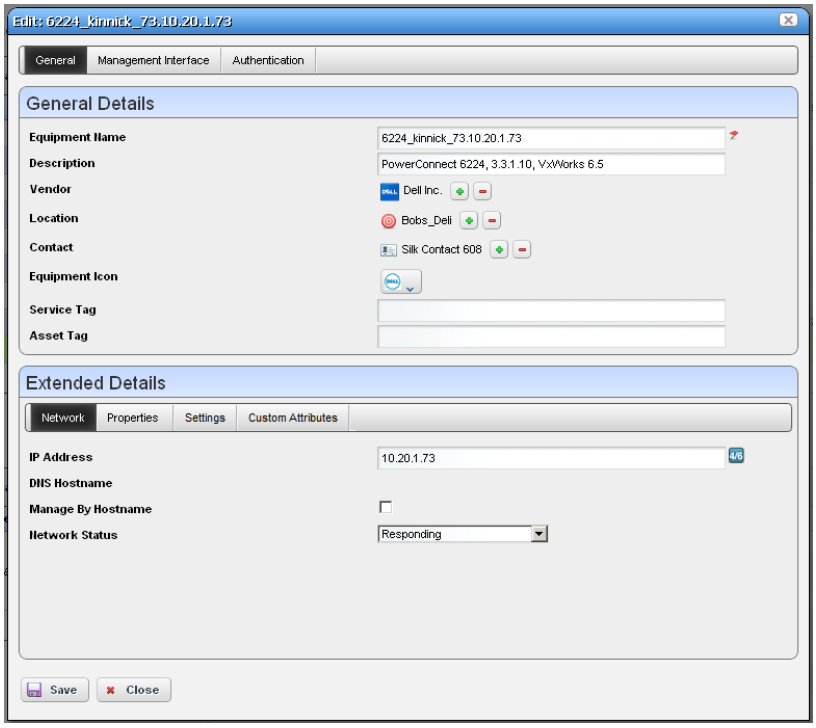
NOTICE

You can edit fields like Notes and Description in subcomponent cards by right-clicking them in the resource tree.

Resource Editor: General

This screen may vary for different kinds of devices. Its *General Details* panel displays the *Name*, *Description*, *Vendor*, *Location*, *Contact*, and *Equipment Icon* for the selected device.





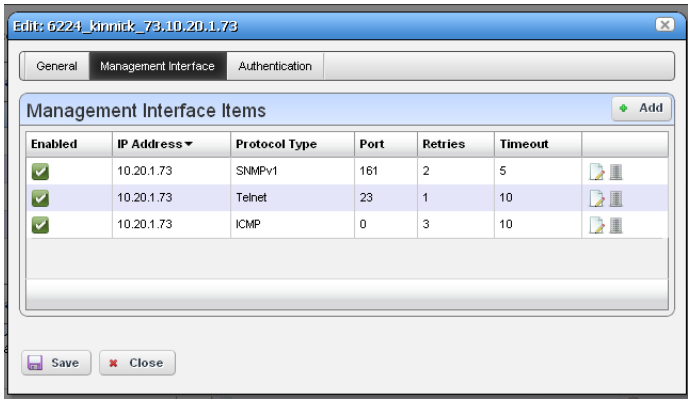
The *Extended Details* panel includes *Network*, *Properties* and *Settings* tabs. These let you view or alter things like *IP Address*, *DNS Hostname*, *Manage by Hostname*, *Network Status*, *Model* and *Equipment Type*, *Serial Number*, *Software Version Firmware* and *Hardware* versions. The *Settings* tab lists the *System Object ID*, *Date created* (the date this managed device entered the database), *Creator* (the user who discovered or created the device), *Install Date*, *Management State State* (see also the *Manage* > *Administrative State* menu below), *Operational State*, *Topology Icon Size (eXtra Large - Small)*, and any *Notes* about the device.

NOTE:

Changing fields in the Editor screens like Network Status, Administrative State, Operational State (and MAC address for ports) do not change the device; they change only the OpenManage Network Manager database. You can alter these fields to take notes or set aspirational values, but no change goes to the device, and resync eradicates changes made if the device has conflicting values.

Resource Editor: Management Interface

This lists the management interfaces for the selected device, including the *IP Address*, *Port*, *Retries*, and *Timeout*.



You can *Add* interfaces with the button in the upper right corner, delete them with the icon to the right of the listed interface.

NOTICE

If an operation produces an error saying the device lacks authentications, if none exists that corresponds to the authentication type, make sure that you add a management interface as well as authentication to remedy that problem.

Resource Editor: Authentication

This lists the authentications for the selected device. You can *Add* authentications with the button in the upper right corner, delete them with the icon to the right of the listed authentication. These originate in the portlet described in Authentications Portlet on page 628.

Details—Displays several tabs with detailed resource information. A reminder of the selected device's name appears above the tab bar. See Connected Devices Portlet on page 538 for more information about this screen.

NOTE:

Not all devices support the options listed below for the *Manage* menu.

Manage > Management State—This lets you select from the following alternatives:

Normal—The device is unconstrained by the other Administrative States. Changing from Suspended to Normal stops alarm suppression. Standard access, and inclusion in right-to-manage count.

Decommissioned—While this device is in inventory, it is not active. No device access allowed, no Monitor associations, no event processing, no Management Interfaces, no Authentication, no links, and no services are permitted.

Suspended—Suspends all device-related activities. No device access allowed, Monitoring Suspended, No event processing, Counts against right-to-manage.

Planned—Planned (future) device. No device access allowed, no monitor associations, and no event processing.

Maintenance—Neither alarms or polling apply to the device. Does allow resync and Adaptive CLI. Standard device visibility.

NOTICE

You can select multiple devices to change their Management State at once.

NOTE:

Write functional permissions control whether the Management State menu item appears in this menu.

Manage > Domain Access Control—Select the Multitenancy domain where the selected device is to be visible, or manageable. This only appears if you have implemented the Multitenancy option. See the OpenManage Network Manager *Installation Guide* for details about that option.

Manage > Configuration—Manage the configuration. (Does not appear for all devices.)

Manage > Maintenance Log—View the maintenance log for the selected device. See Connected Devices Portlet on page 538 for more about maintenance logging capabilities.

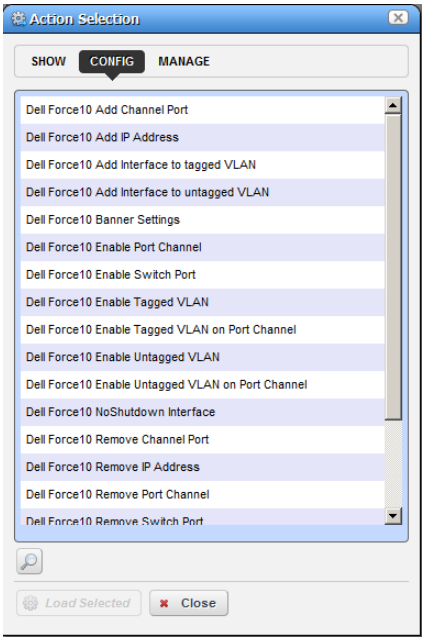
Manage > Control: Reboot—Reboot the selected device.

Manage > Control: Shut Down—Shut down the selected device.

Manage > Factory Reset—Reset the device to factory defaults. Reset now requires two confirmation clicks, and does not support multiple device selection.

Visualize—Create a topology map of the selected resources. See Using Visualization Tools for more about such maps. You can Ctrl+click in the expanded portlet to select several resources, then right-click to display them in a topology map. You can also create Managed Resource Groups Portlet and right-click to Visualize them.

Actions—Actions you can initiate here can include things Adaptive CLI Actions (see), and other



actions specific to the selected device.

Actions (including Adaptive CLI) appear in *SHOW*, *CONFIG* and in some cases *MANAGE* categories. The list that appears depends on the device selected. You can also open search field by clicking the magnifying glass at the bottom of this screen. Using that field, the list narrows to actions matching your search string. Select one, and click *Load Selected* to run it manually.

See Actions Portlet on page 265 for more about configuring these activities.

When you schedule an action (clicking the *Add Schedule* button) through these screens, click *Apply* to accept the schedule. Finally, you must click *Save* in the Action Selection screen after confirming the schedule, or no schedule applies.

NOTE:

Since menu items appear in alphabetical order, this may be in a different location, depending on the device vendor name.

Change Management—Select from *Change Determination* to run that process (see *Change Determination Process* on page 344), *Execute Proscan*, to execute any Proscan policies connected to the selected device, or *Execute Proscan Policy* to execute any Proscan. See *Compliance Policy Summary* on page 324 for more about these.

Adaptive CLI—This displays *Adaptive CLIs* related to the selected device, and opens with a screen where you can enter any relevant parameters for those commands. See the previous *Action* menu item's description, and for more about these.

Direct Access—Direct Access opens a sub-menu where you can select the type access to the selected device. You can ping the device, select a MIB browser or a terminal. See MIB Browser on page 468 and Terminal on page 469 for more the about the available direct access options.

NOTE:

The client must have Java installed (and updated) for direct access to function correctly.

NOTICE

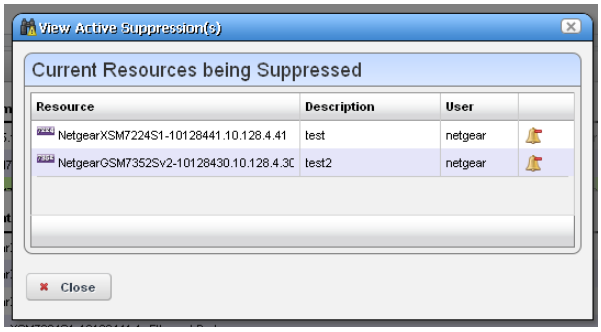
Your ability to open a telnet session with a device typically depends on having the correct telnet/SSH authentication. If you have only partially discovered a device with SNMP, but without telnet/SSH, then direct access telnet connection will not work, nor will Adaptive CLIs. To repair such partial discoveries, edit the device and add the correct telnet authentication *and* a telnet management interface.

Event Management—This lets you suppress or update alarms related to the selected resource. You can *Start Alarm Suppression* (*Stop* appears, once you have started suppression), *Stop All Alarm Suppression*, *Schedule Alarm Suppression*, *View Active Suppression(s)*, View Event History, and *Resync Alarms* (corrects OpenManage Network Manager's display to match the latest information from the device already in the database; device resync does this too, for the selected device). Alarms resync for all devices. This corrects the display when the alarm color displayed, either here or in topologies, does not match the highest severity alarm for the device in the alarm portlet. OpenManage Network Manager issues no alerts when resync occurs.

When you *Start* alarm suppression, first enter a description in a subsequent screen, then a Success / Failure message appears confirming suppression has started.

Schedule displays a *Parameters* screen where you can describe the scheduled suppression and select a duration and any additional suppression targets. The *Schedule* tab on this screen lets you start suppression at a specific time and configure any recurrence, and termination (*Stopping on*) for the scheduled suppression. The termination can either be a date, a number of occurrences or *Never*.

Deleting, stopping or disabling a schedule does not interrupt suppression, once it has started. You must right click selected devices and select *Stop All Alarm Suppression*. You can also delete suppressions after you select *Event Management* > *View Active Suppression(s)*.



The viewer lists devices with active alarm suppression, their description and configuring user. Click the *Stop Suppression* icon to the right of listed devices to terminate their alarm suppression.

Suppressed events / alarms do not appear in the Alarm display, but, unlike rejected events, the Event History screen can display a record of them.

NOTICE

Suppression, as described here, is an excellent way to reduce meaningless alarms during a maintenance period, particularly if you Schedule alarm suppression during your maintenance interval.

If you suppress alarms, a clearing alarm that arrives after suppression begins has no effect on existing alarms. You may therefore need to manually clean up related alarms after stopping suppression. Stopping alarm suppression does not execute any action to change any alarms based on alarms that are no longer suppressed. Visible signs of starting or stopping alarm suppression may take 30 - 60 seconds to appear on the client screen.

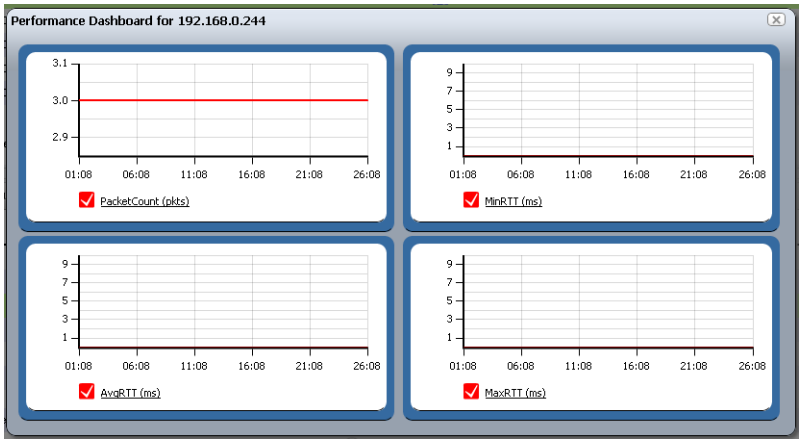
File Management—View a current configuration file, compare it to previous backups, backup, restore, import or export a configuration file. You can also deploy firmware to devices from this menu.

If you go to the Configuration Files portlet, you can also edit backed up configuration files. See File Management Menu on page 582 for details.

Links—Create a new link or discover links between members of the selected group, and others. See New Link on page 532 and Link Discovery on page 533 for details.

Performance—Select from the following options:

Show Performance–This displays a dashboard with various performance metrics for the selected device. These can include packet counts, RTT (round-trip time) measurements, and CPU / Memory utilization graphs.



See Dashboard Views on page 223 and Show Performance Templates on page 232 for more about re-using and managing these capabilities. The default appearance of these performance graphs depends on what monitors you have running.

To remove/hide graphs that appear here, add the a property to `oware/synergy/conf/server-overrides.properties`. For example, `show.perf.exclude=MinRTT,AvgRTT,MaxRTT` conceals RTT graphs. Restart the synergy server for this to take effect. Find the attribute names in the *Calculated Metrics* screen of OpenManage Network Manager's monitor editor.

OpenManage Network Manager has the ability to export performance graph to CSV. There is an export button to each chart in the launched dashboard, when the button is clicked a job is created and a message is created in the My Alerts when the csv file is ready. Clicking on the magnifying glass next to the "Performance CSV report is now ready for viewing" message causes the file to be downloaded.

NOTICE

An alternative way to find attribute names: Invoke *Show Performance*. Click the pencil icon to edit the dashboard. The attribute names appear at the bottom of the screen.

Show Top Talkers–This displays a *Top Talkers Dashboard* of performance metrics for the selected resource. Use the icon in the top right corner to re-configure the default display. Top talkers gets data for the subcomponents of the selected device. Normally you would need the SNMP interface monitor enabled to see top talkers data.

See Dashboard Views on page 223 and Top N [Assets] on page 220 for more information.

Show Key Metrics–This lets you see available key metrics for the selected resource, and configure their display. See Key Metric Editor on page 236 for more.

Resource Groups—This lets you add the selected device to new Dynamic or Static groups, or to existing groups. See for Managed Resource Groups Portlet on page 637 more about this.

Resync—This re-queries the device for more current information, including alarms.

Traffic Flow Analyzer—*Register* configures the selected device to appear in the Traffic Flows displays (see Traffic Flow Analyzer).

Show Traffic displays the traffic flow information for registered devices in an expanded Traffic Flow portlet. This displays Traffic Flow Analysis data that contains the endpoint for the selected device IP (if available) whether or not it is a *Register*ed exporter.

Services—If you have the Service Center option installed, sub-menus let you *Redeploy* and *Undeploy* services for the device. A subsequent selector screen lets you pick the service.

NOTICE

You can also display a *Registered* column in the Managed Resource portlet, and click the heading to sort the Flow exporters to the top of the display.

Delete—Remove the selected device from inventory.

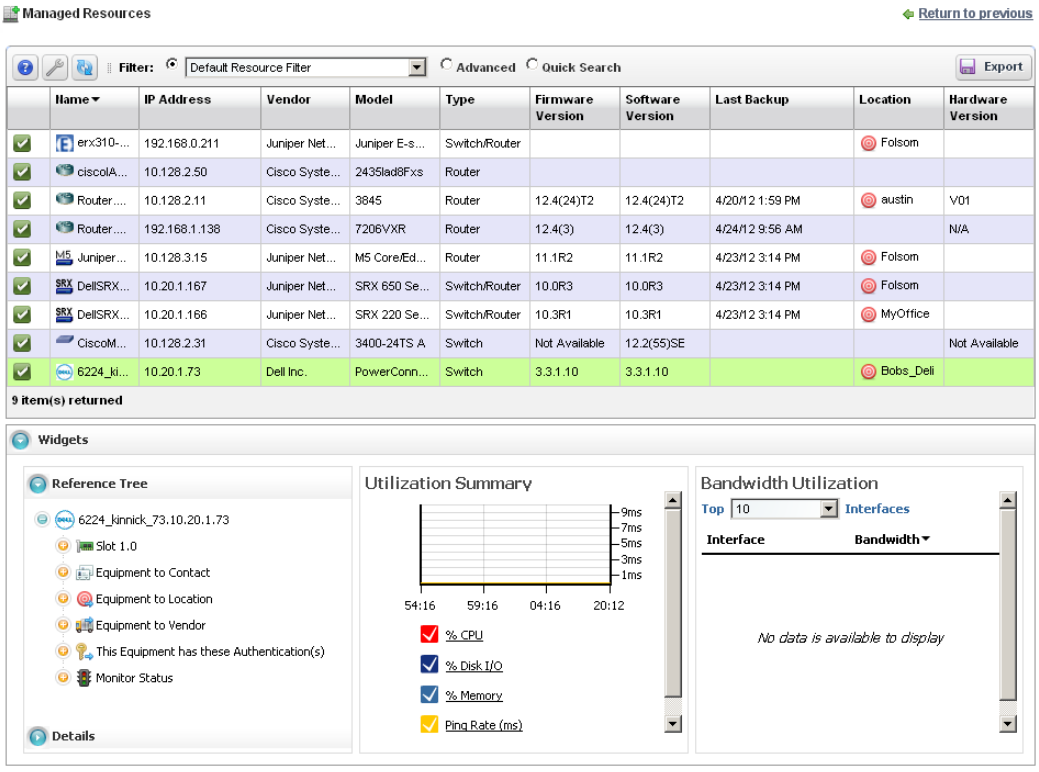
Edit Custom Attributes—Opens the Custom Attribute Editor where you define field characteristics, such as whether it is enabled, the label name, and the tooltip.

View as PDF—Displays the selected device as an Acrobat PDF file.

Share with User—Opens the Share with User window where you select the colleague you want to share the selected rules with and then type your message.

Managed Resources Expanded

If you click the plus (+) in the upper right corner of the summary screen, the expanded portlet appears. As in most expanded portlets, you can limit what appears listed with the filters at the top of the screen. Select the filter from default, seeded filters with the pick list at the top left corner of the screen. You can also create your own custom filter by clicking *Advanced Filter* to the right of this pick list (see Defining Advanced Filters on page 86 for more).



The *Settings* button lets you configure the displayed columns and their order. Menu items are as described in the previous section.

NOTICE

You can select multiple devices by Ctrl+clicking them in the expanded portlet. This lets you do these same tasks on more than one device. You can also perform such tasks on multiple devices with managed resource groups. See Managed Resource Groups Portlet on page 637.

The following are available columns:

Network Status—The status of the resource in the network. For example: *Responding* means this application can, via some network protocol, get the device to respond. *Not Responding* means the device does not respond to the protocol. *Indeterminate* means the monitoring software has not tried to reach the device or there was some other error which prevented us from determining one of the other two statuses.

The appearance of *Network Status* depends on its response to the ICMP monitor. If you disable the monitor (for example, for performance reasons) then a status may appear, but it is not meaningful.

Equipment Name—The name of the device.

IP Address—The IP address of the device.

Vendor Name—The vendor for this device.

Model—The model of the device.

Domain ID—The identifier for the domain of the device.

Service Tag—The service tag of the device.

Equipment Type—The type of equipment.

Firmware Version—The firmware version of the device.

Software Version—The software version of the device.

Last Backup—The device's last backup date and time.

Location—The device's location (with icon).

Hardware Version—The hardware version for the device.

Serial Number—The resource's serial number.

System Object ID—The resource's sysobject ID.

Operational State—The resource's state independent of its network status. Values are:

Disabled—Inoperable because of a fault, or resources are unavailable.

Enabled—Operable and available for use.

Active—Device is operable and currently in use with operating capacity available to support further services.

Busy—Operable and currently in use with no operating capacity to spare.

RTM Category—The resource's right-to-manage category.

DNS Hostname—The hostname of the resource.

Vendor Name—The resource's vendor.

Mediation Server 2 IP Address—The resource's secondary mediation server IP address (applies in a high availability system with two mediation servers).

Contact—Any contact associated with the resource.

Alarm Severity—The highest open alarm for the device.

Last Configuration Change—The time/date stamp for the last configuration change detected.

Registered—Is the resource registered?

Install Date—The time/date stamp for the resource's installation.

Notes—A text field for notes about the resource.

Domain ID—Populated in multitenant environments with the domain.

Asset Tag—Any asset tag identifier for the device.

Creator—Typically the login of the user running discovery to find the resource.

Manage by Hostname—Indicates whether the device is managed by hostname rather than IP address.

Equipment Icon—An icon that represents the resource. You can edit to change this. Discovery assigns standard icons.

Location Name—The location name where the device resides (no icon).

Discovery Date—The date/timestamp for discovery of the resource.

Management State—The management state of the resource.

Mediation Server IP Address—The resource's mediation server.

Last Modified—A time/date for the last modification.

Description—A text field for a description of the resource.

MAC Address—The resource's Machine Address Code.

This bottom of the screen has several snap panels, some compressed "windowshade" style. Click the title bar for these snap panels to toggle expand / collapse. These display information about the device selected in the list at the top of the panel.

Reference Tree

This displays the device and connected components, tree style.

Details: General:

This includes information about the *Equipment Name*, *Vendor*, *Location*, *Contact*, *Icon*, and *its Last Modified* and *Discovery Date*.

Details: Properties

This tab includes the *IP Address*, *DNS Hostname*, *Firmware Version*, *Hardware Version*, *Model*, *Serial Number*, *Software Version*, *Managed by Hostname* (if active, this resolves a DNS name rather than use an IP address to manage this resources), and *Equipment Type* information.

Details: Settings

This includes the *system Object Id*, *Date Created* (that is, discovered), *Creator* (the user who performed discovery), *Install Date*, *Administrative State* (Locked [Device use is prohibited] Shutting Down [Only existing users can use the device] Unlocked [Normal use of device is permitted]), *Operational State* (Disabled [Inoperable because of a fault, or resources are unavailable] Enabled [Operable and available for use] Active [Device is operable and currently in use with operating capacity available to support further services] Busy [Operable and currently in use with no operating capacity to spare]).

OpenManage Network Manager includes a task that updates the operational and administrative states of a port or interface when an event processing rule (EPR) responds to the events listed below. Five new automation EPRs respond to these events and invoke this update task with the target from the entity associated with the event. Only subcomponents are affected. The EPRs are as follows (impacts in parenthesis follow them):

monitorTargetDown (operational state = Down)

monitorTargetUp (operational state = Up)

monitorTargetIndeterminate (operational state = Unknown)

linkDown (operational state = Down, administrative state = the value of the var bind ifAdminStatus)

linkUp (operation state = The value of the var bind ifOperStatus, administrative state = Up)

Utilization Summary

A graph of the device utilization, typically for CPU, Disk I/O, Memory and ping rate.

Bandwidth Utilization

A graph of the device's bandwidth utilization. Notice that you can change the number of top interfaces graphed, when this is applicable.

See also Bandwidth Calculation on page 216.

Direct Access

Direct access provides less-mediated access to the device in the following ways:

- MIB Browser
- Terminal
- Ping (ICMP)
- HTTP / HTTPS

The following sections describe those direct options in more detail.

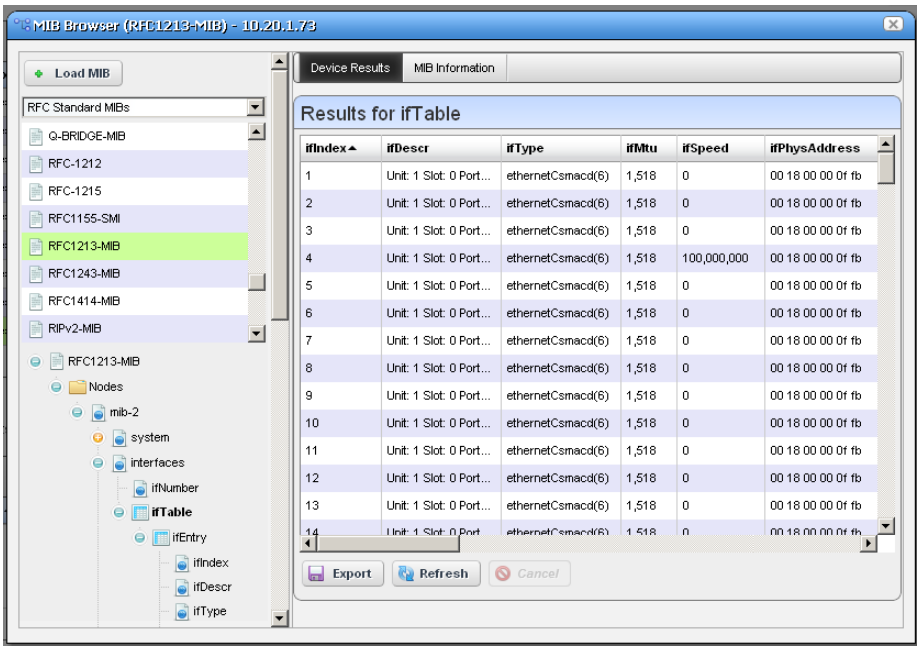


NOTE:

Best practice is to avoid special characters, particularly # and > (command line prompts) in device banners so terminal access is unambiguous.

MIB Browser

As part of the *Direct Access* menu, the *MIB Browser* lets you examine SNMP data available about devices.

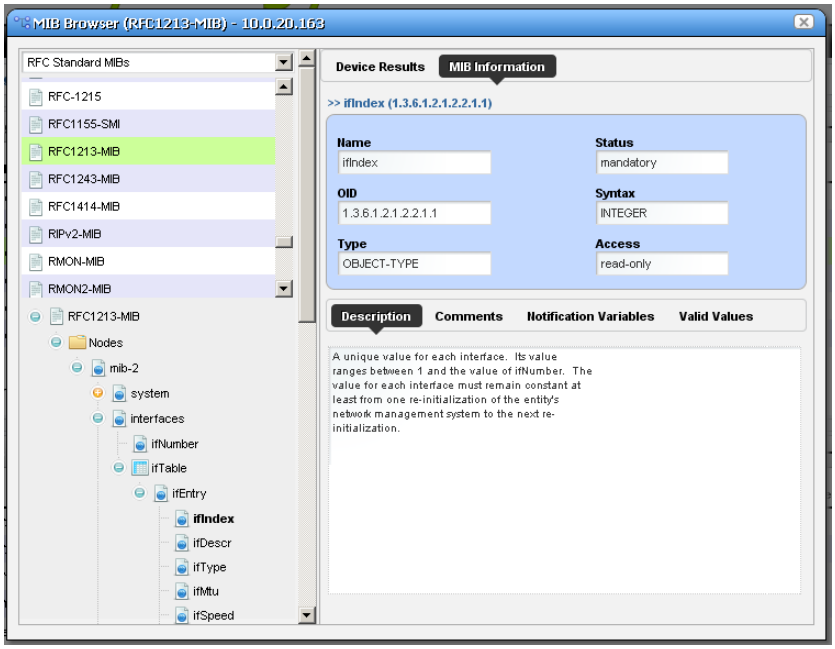


The screen that opens when you select this option displays MIBs available in OpenManage Network Manager in a tree on the left. Notice that a pick list at the top of the left column narrows what appears in the tree. A progress bar at the bottom of this screen indicates a query for the selected information is in progress.

Click *Load MIB* at the top left corner of the screen to load a new MIB. A file selection dialog opens after you click *Load MIB*. Click the *Refresh* button at the bottom of the browser to re-query the device for new information. Click the *Export* button at the bottom of the browser to export the screen contents to a spreadsheet (Excel-format) file.

Use the *Load MIB* button in the upper right corner, or the menu described in Using Extended Event Definitions on page 114 for loading new MIBs.

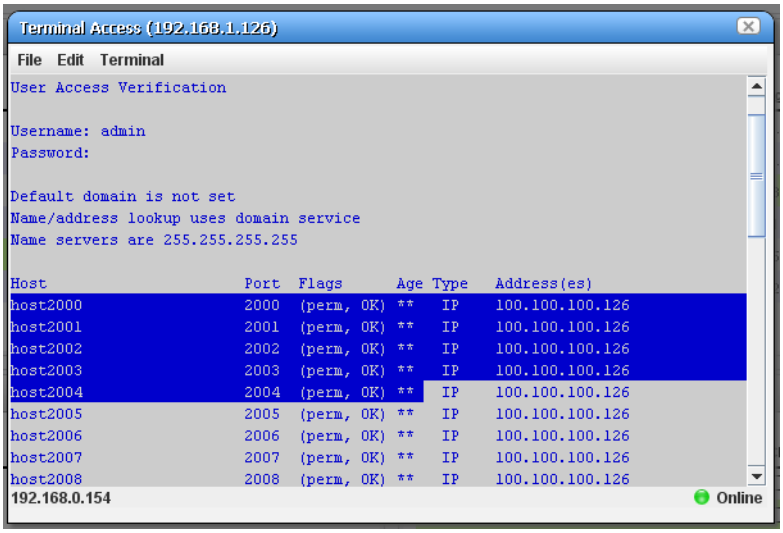
Select a MIB and expand it to see the contents for a selected node appear on the right. In addition to the *Device Results* tab, which displays what the currently selected device uses from the MIB, the *MIB Information* tab displays the parameters available for the selected node.



Notice that the *Description*, *Comments*, *Notification Variables*, and *Valid Values* tabs appear at the bottom of this screen.

Terminal

This opens a terminal shell connected to the selected device.



A green icon in the lower right corner indicates the device is online, while the IP address of the device appears in title bar. The IP address of OpenManage Network Manager's server also appears in the lower left corner, when the connection is active.

The following menus appear for your terminal session:

File—This menu lets you *Connect* or *Disconnect* to the device.

Edit—This menu lets you *Copy* or *Paste* text within the terminal session. Click and drag to select text.

Terminal—This menu lets you set *Foreground* and *Background* colors, as well as configuring the *Font* and *Buffer* sizes. *Reset Terminal* restores the defaults.

Terminal is an applet that requires a Java Runtime Environment be installed and associated to the browser as a plug-in on the client machine. See also Setting Java Security for Terminal Access on page 141 below.

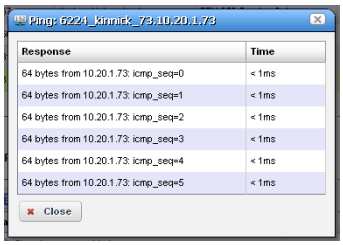
NOTICE

You can cut and paste from the Direct Access terminal.

Telnet sessions are synchronous. You cannot interrupt a command in progress with another command you send, unless you have enabled something that periodically prompts for additional commands (for example enabling line continuation prompts).

Ping (ICMP)

Select this option from the Direct Access menu to initiate ICMP ping, and to display a list of the selected device's ping responses.

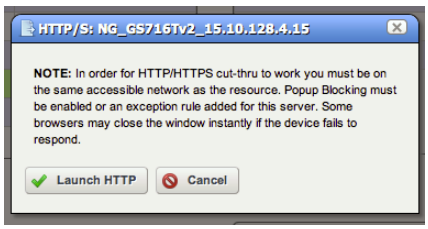


Alternatively, an error message can appear describing the device's lack of response.

When ping responds in less than one millisecond, results appear in a table with <1ms entries.

HTTP / HTTPS

Selecting this menu item opens the default browser, providing access to the selected device.



An intervening dialog appears advising you about the required network conditions for a successful connection.

Secure Connections to OpenManage Network Manager

Typically multi-server installations with load balancers are where OpenManage Network Manager users need secure connections. Consult the *Installation Guide* for instructions about how to configure HTTPS to connect to a load balancer in such an installation.

Quick Navigation Portlet

The Quick Navigation portlet lets you quickly perform some basic tasks:

Quick Discovery—Discover devices in your network with the Quick Discovery defaults, or construct a Quick Discovery profile if none exists. See Discovering Resources on page 138 for details.

Link Discovery—After you have discovered resources, this discovers their connections. See Link Discovery on page 533. This option is visable only if you have write permission.

Backup Config Files—This lets you back up discovered devices' configuration files. Before you can use this feature, you must have servers configured as described in File Servers Portlet on page 593. See also File Management Menu on page 582.

OS Image Upload—Upload firmware updates for devices. See Firmware Image Editor on page 588 for more about these capabilities. This option is visable only if you have write permission.

Deploy OS Image—This deploys firmware updates. To deploy images, you must have File Servers configured, as described above for Backup. See Deploying Firmware on page 154.

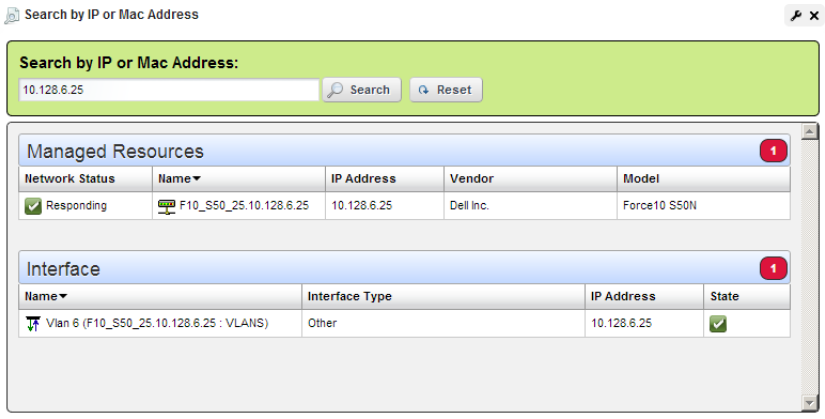
By default, this portlet is available from the Home page. Admin user and Power User can see all the above menu items. The User role sees only options to which the user has write permissions.

Search by IP or Mac Address Portlet

(also located on the Resources page)

Search by IP or Mac Address

This portlet lets you find Managed Equipment, Ports and Interfaces for the IP or MAC address entered.



The same right-click menus as appear in Managed Resources, Ports Portlet or Interfaces Portlet appear in the search results. The display confines those results to what is found; if only ports satisfy the search criteria, then Managed Equipment and Interface do not appear. A count of found items appears in the upper right corner of each panel.

NOTE:

Search by IP or Mac Adress portlet supports search by description on both ports and interfaces

Alarms Page

The Alarms page displays the following portlets by default:

- Alarms Portlet
- Event History Portlet

Access the Alarms page by clicking Alarms from the navigation bar. The Alarms menu provides access to the following sub-pages:

Sub-Page	Description
Alarms by Container	Displays the following: • Alarms Portlet • Container Manager Portlet • Container View Portlet
Automation	Displays the Automation and Event Processing Rules.

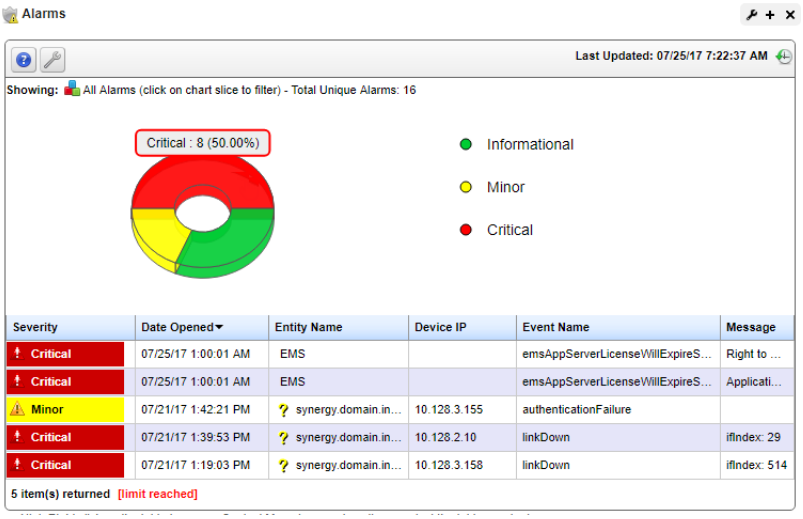
Alarms Portlet

The Alarms portlet on the Home page displays the pie chart and the color legend.

Access the portlet by selecting the Home page, the Alarms page, or the Alarms > Alarms by Container page.

In its summary form, this portlet displays alarms. See General > Entity Change Settings on page 687 for the way to set the summary portlet refresh interval. The default is 40 seconds. If this portlet is on the same page as the Container View portlet, or if it is in expanded mode, refresh does not occur automatically, but you can refresh it manually.

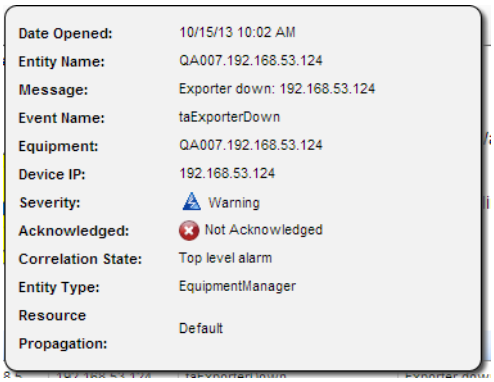
A small clock icon appears in the upper right corner of this portlet if auto-refresh is enabled. A small speaker icon appears if audible alerts are enabled. See Setting Audible Alerts on page 94 for more about this feature.



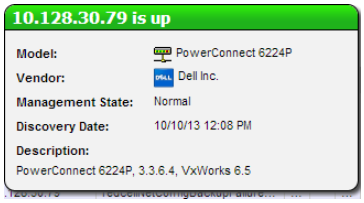
The chart acts as a filter, too. For example, clicking the *Critical* alarms slice means only *Critical* alarms are listed. The chart explodes to highlight the selected slice. Hover the cursor over a portion of the chart and a tooltip with information about that slice also appears. Click exploded slices to return the graph and the list to its original state.

Different tooltips appear when you hover over the Entity Name and Device IP columns. Such tooltips are available if the question mark appears when you hover over the field.

For example, hover over an alarm's entity name and the tooltip displays the alarm's Date Opened, the Entity Name, any alarm Message, Event Name, Alarm and Entity Type, its status as Service Affecting, Notification OID, Equipment, Severity, whether the alarm was Suppressed, or Acknowledged and the Device IP.



Hover over the *Device IP Address* column, and a tooltip appears with information about the alarm source's Model, Vendor, Management State, Discovery Date, and Description, with a title bar that indicates whether the device is running or not. Such tooltips elsewhere also include other device-dependent items. For example, bar graphs to display the % CPU [utilization], % Memory, and Description..



By default, the chart appears only when alarms exist. See the Configuring the Alarms Chart section for options available in configuring the display. See Alarms Menu on page 477 for details about menu items available when you right-click in the summary and expanded portlets.

The following columns appear in this screen by default:

Severity—The alarm severity indicated by the color of the leftmost icon. The severity only has meaning for Alarms and Security Alarms. Informational Alarms get a severity level of Indeterminate. Closed alarms appear without color.

Date Opened—The date the alarm appeared.

Entity Name—The entity emitting this alarm (often within the Equipment).

DeviceIP—The IP address of the equipment where the alarm appeared.

Event Name—The event associated with the alarm.

Message—The message associated with the alarm.

Open the *Settings* > *Columns* screen to see additional possibilities for columns.

If an alarm is **Service Affecting,** (reflect an impact on a service) it propagates to appear as components of service- and customer-related alarms. Service-Affecting alarms are of indeterminate or greater severity. The Service Affecting alarm column in this portlet does not appear by default. To see an alarm's propagation, show that column in the Using Extended Event Definitions portlet, where it is concealed by default.

NOTICE

You can select multiple rows in the Alarms portlet and the Managed Resources portlet. Many other columns are available, including those related to suppression, region, any parent alarm, and so on.

See Alarms in Visualizations/Topologies on page 530 for a description of how alarms appear in the topology portlet. The Expanded Alarm Portlet section below describes additional alarm portlet capabilities.

Configuring the Alarms Chart

In the summary Alarms Portlet, *Settings* let you select an Alarm Chart, the expanded Alarms portlet's totals, or no chart. The last two permit selecting a filter. The Alarm Chart *is* a filter itself. If no data exists for the chart and the Chart option is on, the portlet returns to "no-chart" mode.

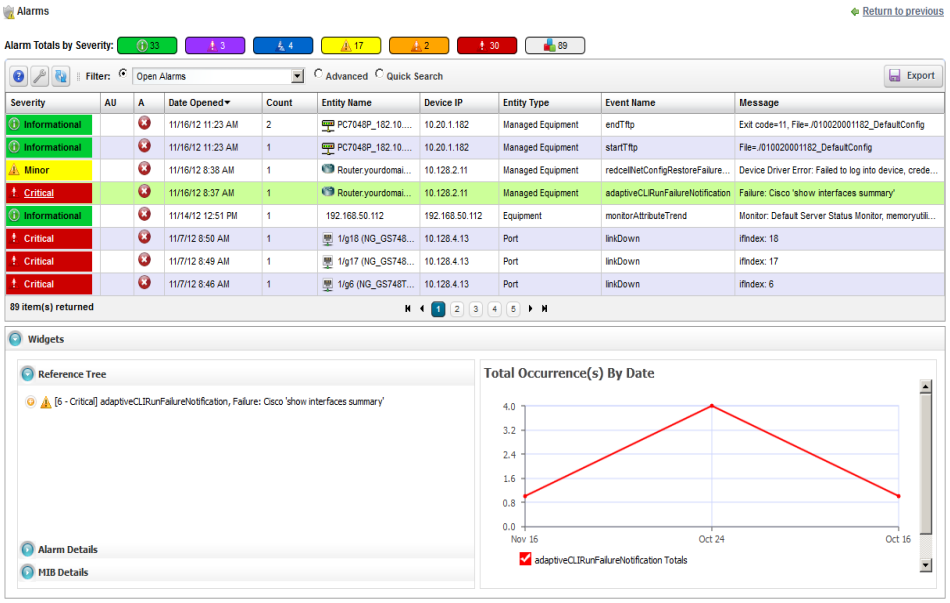
Settings persist if you have Admin rights or the Portlet is on your Public/Private pages (like standard behavior).

NOTE:

Changes appear after you click *Apply.* The *Filter* panel disappears when you select the *Show Chart* option.

Expanded Alarm Portlet

The expanded Alarm portlet appears when you click the plus (+) in the top right corner of the smaller screen.



This displays listed alarms, totals by severity for alarm types found, and Snap Panel details of a selected alarm. By default this screen adds the first of the following columns to those visible in the Event History Portlet summary view. To add the others listed here, right click, and select *Add Columns* to change the screen appearance.

NOTE:

All severity totals appear in expanded view. This display updates automatically when alarms clear.

The following are available additional columns, besides the default columns visible in the Alarms Portlet summary portlet:

Assigned User—The user currently assigned to this alarm (right-click to do this). The assigned user can then look for alarms by consulting the Assigned User (AU) column in the display (concealed by default), or by filtering alarms using Advanced Filters. One can even create an alarm portlet that filters for a single user's assigned alarms.

Acknowledged—*True* or *False*.

Count—A count of the instances of the alarm. Multiples of the same alarm appear as a single row, but increment this count.

Entity Type—The type of monitored entity.

Alarm State—The state (open / closed) of the alarm.

Date Cleared—The date and time that the alarm was closed.

UpdateDate Time—The time stamp for when this alarm was updated (for an additional count, the time the last duplicate was received).

Notification OID—The identifier of the notification displayed as an alarm.

Equipment—The name for the entity emitting the alarm.

Date Assigned—The date and time that the alarm was assigned.

Ack Time—The time the alarm was acknowledged.

Cleared By—The user who cleared the alarm.

MIB Text—The alarm's MIB Text.

Location—The alarm's location.

Suppression Date—The alarm's date / time of beginning suppression, if applicable.

Correlated Time—The alarm's date / time of correlation to a parent alarm (caused by or blocked by).

Suppression End—The alarm's suppression termination.

Entity Description—The description of the alarmed entity.

Region—The alarm's region.

Resource Propagation—Any propagation for this alarm.

Suppressor—The alarm that suppresses this one.

Equipment—The equipment emitting the alarm.

Ack By—The user that acknowledged the alarm.

Correlation State—The role this alarm plays in any correlation (for example: *Top level alarm*, *caused by parent*, *Blocked by parent*).

Has Children—Red for no or green for yes: an indication of whether the alarm has children (see Parent / Child Alarm Correlation: Alarm Details Panel on page 479).

Notes—A text field to take notes about the alarm.

Parent Alarm—The name of the parent alarm (see Parent / Child Alarm Correlation: Alarm Details Panel on page 479).

Domain ID—The Multitenant domain ID emitting the alarm.

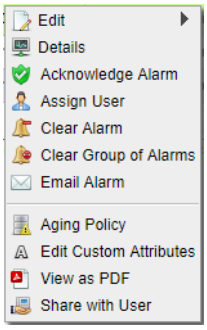
Service Affecting—Red is no, green is yes. Whether this alarm is on equipment in a provisioned service.

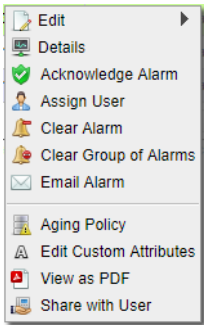
Correlated By—The name of the user who correlated this alarm to a parent.

Suppressed—Red is no, green is yes. Whether this alarm is suppressed.

Rather than filtering with the pie graph, the expanded portlet lets you either the pick list at the top left, or create custom filtering by clicking *Advanced Filters*.

Alarms Menu





Right-clicking an alarm lets you select from the following menu items:

Edit—Access the editors for the Alarm (see Alarm Editor on page 481) or *Event Definition* (see Event Definition Editor on page 498).

Details (Shift+Click)—Open a Details screen for the alarm itself, not the entity emitting it. (see Connected Devices Portlet on page 538 for an example of this type of screen). This contains information like the MIB text, any Event Processing Rules invoked, and a Reference Tree for the alarm. It also lets you configure alarm correlation. See Parent / Child Alarm Correlation: Alarm Details Panel on page 479.

Visualize—Display a topology map that includes the selected alarm(s). See Using Visualization Tools for more about these maps.

Acknowledge/Unacknowledge Alarm—Acknowledges the selected Alarm(s). The current date and time appear in the Ack Time field. Unacknowledges previously acknowledged alarm(s), and clears the entries in the Ack By and Ack Time fields. The red "unacknowledged" icon appears in the expanded portlet and turns to a green check "acknowledged" icon the alarm has been acknowledged.

Assign User—Assign this alarm to one of the users displayed in the sub-menu by selecting that user. An icon also appears in the expanded portlet indicating the alarm has been assigned to someone.

Clear Alarm—Clearing the alarm removes the alarm from the default alarm view and marks it as a candidate for the database archiving process (DAP). Essentially it is an indication to the system that the alarm has been resolved/addressed. If your system has enabled propagation policies, clearing recalculates dependent alarms.

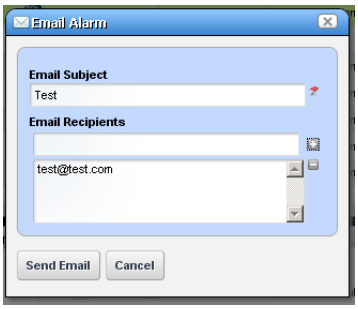
Clear Group of Alarms —Sometimes you might have lots of open alarms that are unimportant because they are old and/or of low severity. For example, perhaps you want to clear all alarms that are informational and are more than a week old. Rather than having to clear them all individually, you can clear them as a group. Before selecting this menu item, you will need to create a filter for the group of alarms that you want to clear. When this menu item is selected, a panel will appear that contains all previously saved alarm filters. When you select a filter from the list and push Execute, it will clear all open alarms that meet the criteria of this filter.

CAUTION:

The Clear Group of Alarms action is irreversible.

Direct Access—Open an SNMP Mib Browser to the alarmed device, a CLI Terminal (Telnet window) to the alarmed device, or ICMP Ping the device alarmed. Only those available appear in the subsequent menu.

Email Alarm—E-mail the alarm. Enter a subject an e-mail address to which you want to mail the alarm's content, and click add (+) to the list of addresses (the minus deletes them). Then click *Send Email*. Click *Cancel* to end this operation without sending e-mail. SMTP setup is required to e-mail an alarm. See SMTP Configuration on page 626 for instructions about setting up e-mail from OpenManage Network Manager. See Alarm Email on page 480 for an example of what the content looks like.



Show Performance—If the equipment is monitored, this displays a performance dashboard for the alarmed equipment. See Dashboard Views on page 223 for more about these.

Aging Policy—This lets you select a policy that determines how long this alarm remains in the database. See Implementing DAP on page 38 for information about configuring such policies.

Edit Custom Attributes—Opens the Custom Attribute Editor where you define field characteristics, such as whether it is enabled, the label name, and the tooltip.

View as PDF—Create an Acrobat PDF document containing this alarm's contents as displayed in the summary portlet basic columns.

Share with User—Opens the Share with User window where you select the colleague you want to share the selected rules with and then type your message.

NOTE:

To resync alarms—that is, query the device for its alarm state—resync the device.

Alarm Snap Panels

These include the following:

Alarm Details—The source, *Severity*, *Message*, *Date Opened*, and so on. See also Parent / Child Alarm Correlation: Alarm Details Panel below.

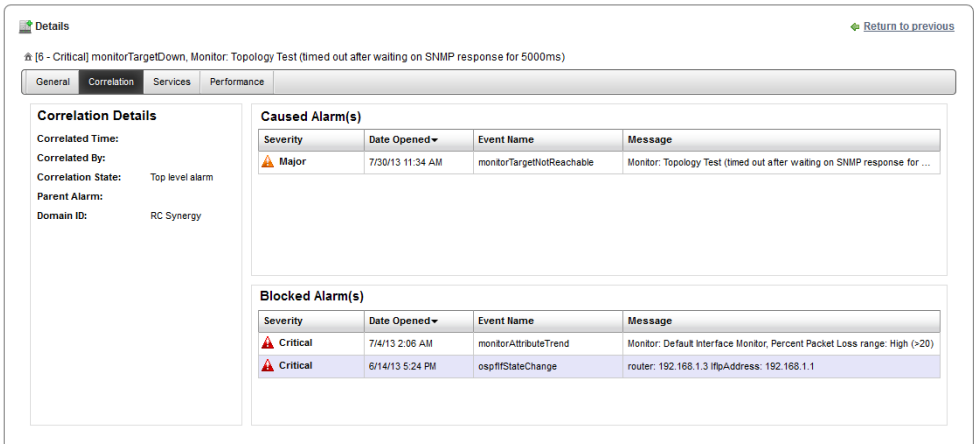
MIB Details—The *Notification OID*, and *MIB Text* for the selected alarm.

Reference Tree—The connection between the alarm and its source in tree form.

Total Occurrences by Date—A graph of the total occurrences of this alarm, by date.

Parent / Child Alarm Correlation: Alarm Details Panel

Like many other items managed by OpenManage Network Manager, Alarms have a Details panel (see Connected Devices Portlet on page 538, for example). In addition to the items mentioned above, the Alarm Details also have a *Correlations* panel.



Alarm parent/child correlation lets you correlate one alarm to another so you can conceal the child alarm(s) in standard alarm views. You can also correlate one alarm to block resolution of another. In effect, parent alarms conceal (or block) correlated child alarms. This can confine alarms that appear or resolve to those requiring action only.

The *Correlations* panel lists the following:

Correlation Details—The current correlation state of the current alarm. Attributes include: *Correlation Date*, *Correlated By*, and *Correlation State* along with information about the correlated, parent alarm. In addition to manually removing the correlation, you can right-click in this component to navigate to the details of the correlated alarm.

Caused Alarm(s)—The alarms caused by this alarm. Right-click to add alarms to the table or to remove them.

Blocked Alarm(s)— The alarms that are currently blocked from resolution by this alarm. Right-click add alarms to the table (and remove them).

When adding a correlated alarm, you can select any alarm that does not already have a parent alarm, then click *Done* to make it a child alarm.

When you correlate correlating one alarm to another, OpenManage Network Manager understands their correlation state as either *Caused By* or *Blocked By*. By default, the correlation state is *Top Level Alarm*.

OpenManage Network Manager does not support multiple correlation states so one alarm cannot be both *Caused By* and *Blocked By*. However, a parent alarm can have both *Caused By* and *Blocked By* child alarms. A single alarm can also be both parent and child. Consider, for example, an alarm that causes several other alarms but is *Blocked By* another alarm. Its parent alarm would appear in the *Correlation Details* panel too.

Alarms correlated as *Caused By* clear automatically when the parent alarm clears. *Blocked by* alarms status as child alarms disappears when their parent alarm clear. This means they become visible again within the alarm view's i.

Alarm Processing Effects

An alarm's correlation state does not affect alarm processing behavior. So if a clearing event enters OpenManage Network Manager, the open alarm clears regardless of its correlation state. Event counts also continue to increase as duplicate events arrive.

Default Filtering

By default all alarm filters exclude child alarms. A filter criteria (*Include child alarms*) can include child alarms, so you can always see all alarms regardless of their correlation state by selecting the *Include child alarms* attribute within the expanded alarms portlet and setting the search criteria to *Is true*.

Additional Alarm Attributes

The following attributes reflect the correlation state for an alarm. When another alarm conceals the child alarm (or blocks it), it sets the following too.

- Correlated By: User who created the correlation.
- Correlation Date: Date the correlation was created
- Correlation State: CausedBy or BlockedBy
- Parent Alarm.
- Has Children: Whether the alarm has children

Alarm Email

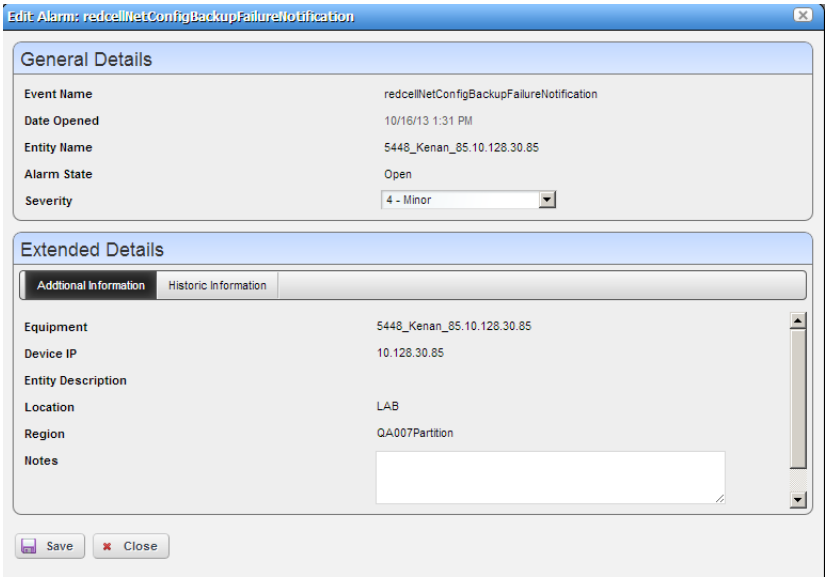
The e-mail sent by right-clicking an alarm has the subject specified when you send it, and contains the information within the alarm. For example:

```
Alarm: monitorIntervalSkip
Alarm Attributes:
==============================
Device IP          =
Message            =
Alarm State        = Open
Severity           = 5 - Major
Count              = 1
Date Opened        = Tue Dec 14 22:01:30 PST 2010
Update Date/Time   = Tue Dec 14 22:01:36 PST 2010
Entity Name        =
Entity Type        =
Entity Description =
Equipment          =
Region             = SUPDEMOPartition
Location           =
```

```
Assigned By          = OWSystem
Date Assigned        = Thu Dec 16 10:40:24 PST 2010
Assigned User        = qatester
Acknowledged         = false
Ack By               =
Ack Time             =
Cleared By           =
Date Cleared         =
MIB Text             = Monitor session was skipped due to resource
   constraints.  Typically, this implies one or more monitors should run
   less frequently.  This may also be caused by a large number of timeouts
   which force executions to take longer to complete than normal.
Advisory Text        =
```

Alarm Editor

The Alarm Editor window appears when you right-click an alarm and select *Edit Alarm* from the Alarms Portlet portlet.



You also have the option to edit the Event Definition (see Using Extended Event Definitions on page 114) or open the alarmed device's Details panel (see Connected Devices Portlet on page 538). The Alarm Editor window contain the following type of information:

Information Type	Provides
General Details	**Event Name**—The event that triggered the alarm. **Date Opened**—The date the alarm occurred. **Entity Name**—The entity emitting this alarm (often within the Equipment). **Alarm State**—The state of the alarm (Open / Closed). **Severity**—The alarm severity indicated by the color of the leftmost icon. The severity only has meaning for Alarms and Security Alarms. Informational Alarms get a severity level of Indeterminate. Closed alarms appear without color. If you change the severity, you may have to refresh the portlet after you save the changed alarm.

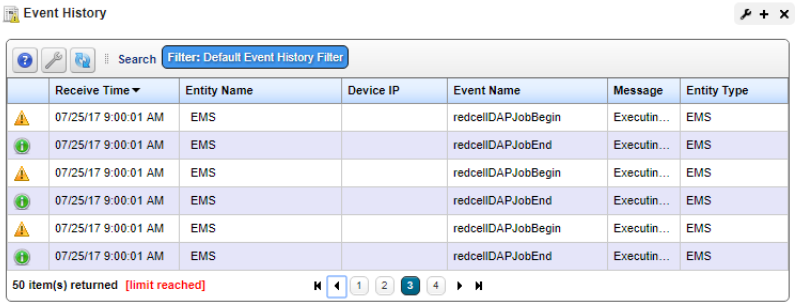
Information Type	Provides
Extended Details: Additional Information	**Equipment**—The equipment (not subcomponent) that triggered the alarm. **DeviceIP**—The IP address of the equipment where the alarm appeared. **Entity Description**—A description of the triggering equipment. **Location**—The location for the alarm. See Locations Portlet on page 644. **Region**—The partition / region for the alarm. **Notes**—A field where you can enter text.
Extended Details: Historic Information	This panel contains primarily read-only fields describing the alarm, including whether it was ***Acknowledged, Ack by, Ack Time, Count*** and so on.
Extended Details: Custom Fields	If you have created any Custom Fields for Alarms, this panel appears in the editor. See Editing Custom Attributes on page 88 for instructions about these.

Event History Portlet

Access the portlet by selecting the Home page, the Alarms page, or the Alarms > Alarms by Container page.

Event History

Not all events appear as alarms. Event History preserves all event information for your system.



The initial portlet view displays an icon whose color reflects any alarm state associated with the event. It also displays the Receive Time, Entity Name, Device IP, and Event Name, Message, and Entity Type. Right-click to edit event definition or entity details, view event details, view or modify aging policies, create a PDF, or share and event with users.

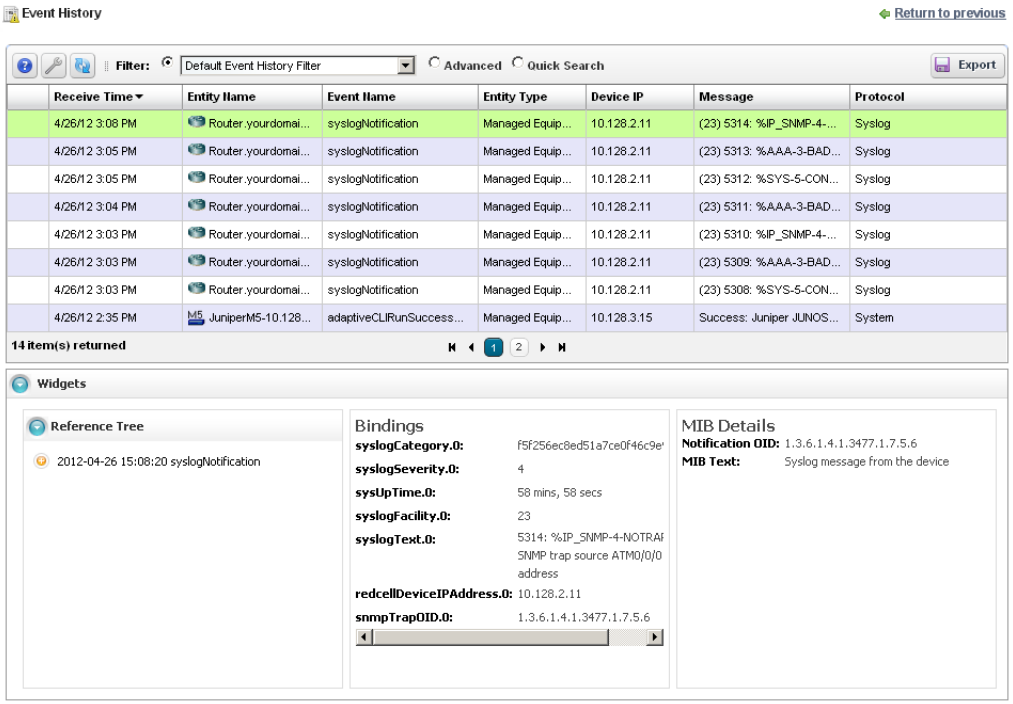
NOTICE

Hovering over the *DeviceIP* column produces a tooltip similar to the Alarms tooltip.

The default filter for this portlet displays only recent events. If you do not see the desired events, expand the period for which they appear.

Expanded Event History Portlet

Clicking the plus (+) in the upper right corner of the initial portlet view displays the expanded Event History. As in other expanded portlets, use the filtering capabilities to further limit the events listed.



The expanded view has columns similar to those described in Alarms Portlet on page 454 or Expanded Alarm Portlet on page 475. Configure these as visible or hidden by clicking *Settings*. The following are some additional columns available.

Receive Time—The date the event was received.

Entity Name—The entity emitting the event.

Event Name—The event identifier.

Entity Type—Typically something like *Managed Equipment*.

Protocol—The protocol that delivered the event. Frequently: *System*, indicating OpenManage Network Manager itself delivered it.

Instance ID—The instance identifier for the event.

Mediation Server IP—The mediation server retrieving the event. If you have a single-server environment, this is blank. It is most useful in a clustered environment.

Location—The location of the entity emitting the event.

Equipment—The equipment emitting the event.

SubType—A classification for the event. For example: *Trap*.

Notification OID—The object identifier (OID) for the event type.

Source IP—The source of the event's IP address.

Region—The region emitting the event.

Event History Snap Panels

Click a listed alarm to display its details in the Snap Panels. The *Reference Tree* displays the event's relationship to any alarms, and to the source device. Click the plus (+) next to an item in the tree to unpack it.

The *Bindings* Snap Panel displays the event's varbind information, including the trap OID, the device's IP address, and other event-specific information.

The *MIB Details* Snap Panel includes MIB information like the Notification OID and MIB Text.

You can right-click the listed events and *Share with User* (see *Sharing a Resource* on page 87), or Modifying Column Settings on page 85.

Rule Editor

After you select a category and type for a new rule, the following screens manage the event processing described in brief in the Creating Event Processing Rules on page 95. The following screens and fields appear in this editor.

- General
- Filtering/Settings
- Syslog Escalation Criteria (for Syslog Escalation)
- If explicit membership is enabled, then you can click Add and this displays a screen through which you can select an explicit member entity and optionally configure specific overrides that would be associated with this member. (for automation rules)

Rules Referring to Subcomponents

Subcomponent names must cache on the server if you want to refer to them in rules. For example, if you want e-mail whenever a linkDown occurs on a port, then you must cache subcomponents. If you cache subcomponents, it impacts performance, which is why such caching is disabled by default.

To enable caching, set the following property in installed.properties:

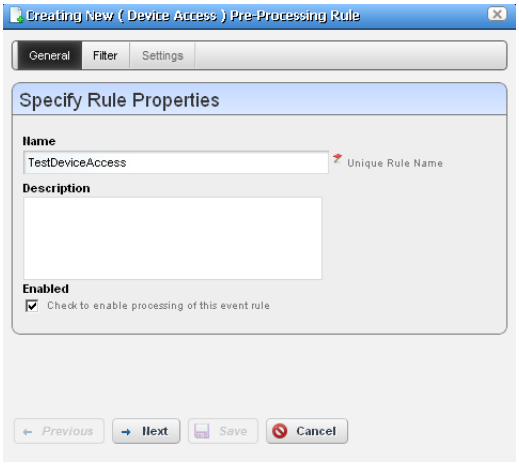
```
com.dorado.redcell.inventory.equipment.subcomponent.cache=true
```

...then restart application server.

The following sections describe editing rules in more detail.

General

The General screen is common to all rule types.



It contains the following fields:

Name—Enter a text identifier for the rule.

Description—Enter an optional text description of the rule

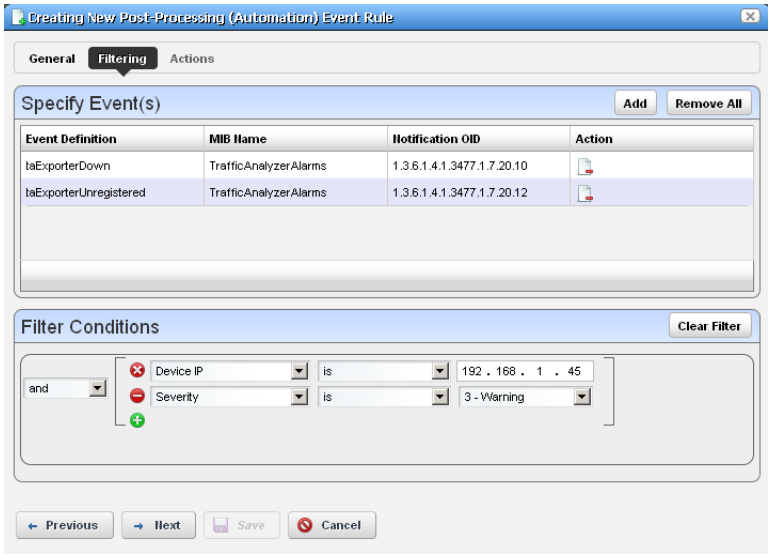
Alarm Only—Visible only in automation rules. Check this to enable the rule only if an alarm is generated, not suppressed.

Explicit Membership — Visible only in automation rules. This indicates that this rule has explicit membership. If any explicit members are defined for a rule, then the event must be associated with one of these entities in order for this rule to execute. This box must be checked in order to enable the buttons to add entities on the Explicit Members tab.

Enabled—Select this option to enable the rule.

Filtering/Settings

For all rule types, select the *Event Definition*. Click *Add* to open a screen where you can select events to include in the event you are creating. This includes a filter at the top that you can use to search for specific events. For example: *Event Name Contains*. You can then click *Add Selection* to include selected items in this filter, or *Add All* to include all displayed events. After you finish event selection, click *Done* at the bottom of this selection screen.



Click *Add Filter* to further filter the selected events. See Defining Advanced Filters on page 86 for more about this feature. After you *Add Filter* the button changes to *Clear Filter* so you can remove any filter from the event rule.

NOTICE

OpenManage Network Manager supports multiple IP addresses per resource. During event processing, filters that include IP address criteria may behave incorrectly when OpenManage Network Manager evaluates the filter. Best practice is using resource name(s) instead of IP addresses.

The following are processing rule types, and a description of their properties.

Protocol Translation— These rules define how to translate messages that are received from protocols other than SNMP into a format that is more similar to an SNMP trap so that they can become events in OpenManage Network Manager. SNMP traps always have all of the data in their payload contained within variable bindings, and this is also the way events are structured within OpenManage Network Manager so for the system to be able to have events that come from protocols other than SNMP, they first have to undergo this translation. Currently the only rule type within this category is *Syslog Escalation*, and rules of this type translate incoming syslog messages into a payload that is more similar to an SNMP trap so that they can become events based on the definition syslogNotification.

Stream Based Correlation — These rules allow you to control the stream of events that are processed. You can do this by specifying a correlation pattern that the system should detect among the events within the stream and then also specifying the action that the system should take to modify the stream in some way. Correlation patterns can take into account the frequency of certain types of similar events (as is the case for *Frequency Threshold* rules) or they can operate on the intermittent fluttering of the raising and clearing of certain types of

alarms (as is the case for *State Flutter* rules). You can use rules of types within this category for the purpose of minimizing the number of events submitted to the application server for further processing.

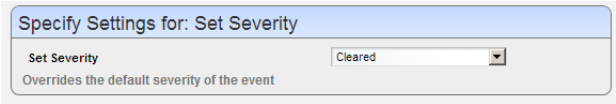
Event Definition Override — By default, events inherit all of their attributes (such as severity, behavior, etc.) directly from the event definition identified by the notification type OID. These rules allow you to override the default attributes such as severity (*Set Severity*), service affecting (*Set Service Affecting*), and/or behavior (with rules of the type Reject Event or *Suppress Alarm*). *Device Access* rules also fall into this category because you can use rules of this type to normalize the device-specific events into standardized events.

Automation— These rules execute specified actions for the rule after the event processing occurs. Note that Automation is both a rule category and a rule type since there is only one type of rule within this category.

The following are *Event Definition Override* rule types:

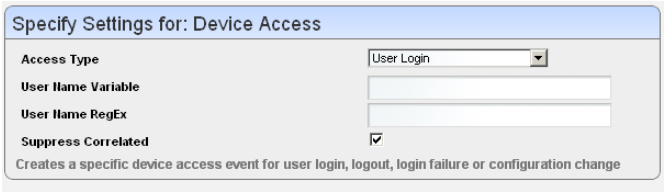
Reject Event — This screen presents the Specify Event Filtering portion of the screen without any Settings in the lower screen. Specify events to reject with this selection and filtering.

Set Severity — This rule overrides the default alarm severity of an event selected and filtered in the upper screen.



Suppress Alarm — This screen presents the Specify Event Filtering portion of the screen without any Settings in the lower screen. Specify events/alarms to suppress with this selection and filtering.

Device Access—The Device Access example creates a specific device access event for user login, logout, login failure or configuration change. Select the *Access Type* (*Config Change*, *Login Failure*, *User Login*, *User Logout*) from the pick list for that field.

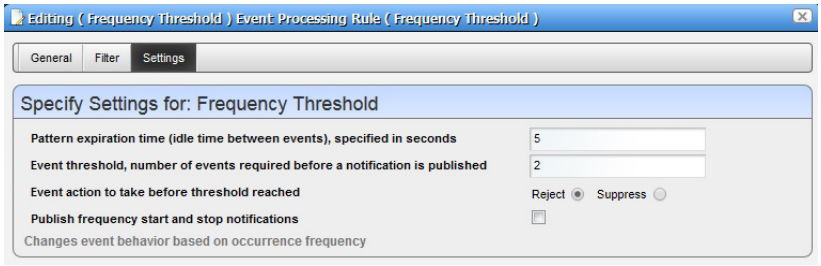


Enter the *User Name Variable* and/or *User Name RegEx* match string in those fields. This confines rule response to the selected users.

Select *Suppress Correlated* events if you do not want to see events correlated with this one.

The following are *Stream Based Correlation* rule types:

Frequency Threshold—This rule type changes event behavior based on the frequency of the selected event. For successive events of the same type, associated with the same entity, it suppresses or rejects the first few received, up to the given event threshold, within the pattern expiration time, and publishes the rest.

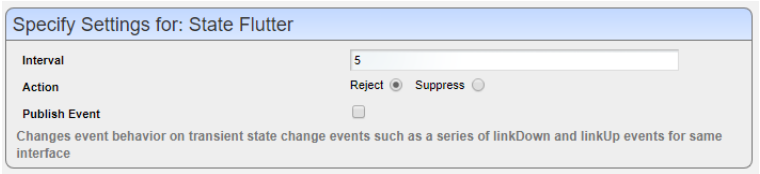


Enter the *Pattern expiration time (idle time between events), specified in seconds* and *Event threshold, number of events required before a notification is published*, then select an *Event Action to take before the threshold is reached* (*Reject* or *Suppress* the event). If you *Reject* an event, it does not appear in Event history; if you *Suppress* it, it creates no alarm, but it does appear in the Event history. Check *Publish frequency start and stop notifications* if you want OpenManage Network Manager to keep a record of when this rule starts and stops filtering events.

On receipt of the first event matching the given filter criteria, OpenManage Network Manager enables the selected pattern. It remains active until no matching events are received for at least the number of seconds specified as the pattern expiration time. The rule always waits this number of seconds before publishing the event(s), even if the number of matching events crosses the threshold before the pattern expires. Every time the rule reaches its threshold in this time window, it publishes one event and then reset the counter.

For example, consider a pattern configured for 3 events in 10 seconds. If OpenManage Network Manager receives only 2 matching events in a 10 second time window then it publishes no events. With these same parameters, if OpenManage Network Manager receives at least 3 but less than 6 (3 times 2) events, then OpenManage Network Manager publishes one event. If it receives six events then it publishes two events (because this amounts to 3 times 2).

State Flutter—This type of rule changes event behavior on transient state change events like a series of LinkUp and LinkDown events for the same interface. For successive raising and clearing events of the same type and associated with the same entity, it publishes the final state in after a given number of seconds has elapsed and it suppresses or rejects the extra events.



After you select the event and filtering, enter the *Interval* (seconds), the *Action* (*Reject* or *Suppress* the event). If you *Reject* an event, it does not appear in Event history; if you *Suppress* it then it creates no alarm but it does appear in the Event history. Check *Publish Event* if you want OpenManage Network Manager to keep a record of when this rule starts and stops filtering events.

OpenManage Network Manager always publishes the first raising event matching the given filter criteria. If OpenManage Network Manager receives a correlated clearing event within the given number of seconds then this activates the State Flutter rule pattern. Until the pattern expires, it holds all correlated rising and clearing events. This way if the state goes from rise to clear and back to rise in rapid succession, the result will be the final state after the number of seconds has elapsed, but without publishing the extra events and/or creating the alarms.

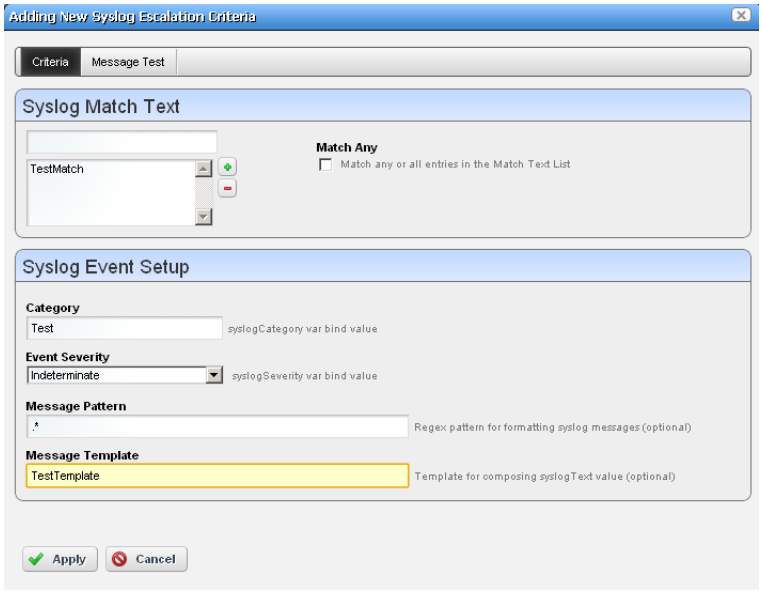
The following are the *Protocol Translation* rule types:

Syslog Escalation —This screen presents the *Specify Event Filtering* portion of the screen without any *Settings* in the lower screen. Specify events to select. Then click *Next* to go to the *Escalation* tab.

Automation rules let you modify the *Specify Event Filtering* portion of the screen without any *Settings* in the lower screen. Specify events to select. Then click *Next* to go to the *Actions* tab. See Actions on page 493 for more about that feature.

Syslog Escalation Criteria

This tab of Syslog Event Rules lets you manage events based on matching text, and configure messages in response to such matches.



Criteria: Syslog Match Text

In this tab, enter the Syslog Match Text. Click the plus to add matching text to the list below the empty field. There are two options for *How to Apply the Match Text to Syslog Messages*, which is controlled by whether or not this box is checked. Check to match any single entry (only one message match text must be present in the message) or uncheck to match all entries (all message match texts must be present). For example, consider that the Message Match Text list contains the following entries: "LOGIN" and "FAILED" and consider a Syslog message that says "USER LOGIN SUCCESS". This message would be a match if the box was checked but it would not be a match if the box was unchecked. If the list contains the same entries but the Syslog message was "USER LOGIN FAILED" then this would be a match regardless of whether the box was checked.

Criteria: Syslog Event Setup

This portion of the Criteria screen sets up the `syslogNotification` event emitted when matching occurs. Here are the fields:

Event Severity — Select the alarm severity of the event emitted when a match occurs. You can choose to assign a specific severity to the syslogNotification events that would be created from this escalation, such as Major, Minor, etc., or you can instead select Indeterminate, which will use the severity within the original Syslog message to determine the severity of the resulting event. For example, if you select Indeterminate and the Syslog message has a severity of Critical then the resulting event will also be Critical. But if you select a specific severity from this drop down, such as Minor, then this the events will be assigned this severity regardless of what severity is found within the original message.

Message Pattern —- An optional regular expression for the text to retrieve and transmit in the created event's varbinds. Syslog escalation uses the retrieved value(s) entered in the template fields to populate the associated varbinds.

Category Template —A directive for how to populate the syslog category varbind value. This is a template field, which means that you can either enter static text (like `Category1`) or a template containing variables (like `Category%1`). This populates the `syslogCategory` varbind with the appropriate text, for example: `Category-LOGIN`. See Template Fields below for more about this type of field.

NOTICE

When you dynamically populate the syslog category, you can more easily base extended event definitions (EEDs) on the `syslogNotification` definition. For example you could change the base event definition to allow EEDs on the syslog category varbind. See Using Extended Event Definitions on page 114 for more about EEDs.

Message Template— A directive for how to populate the syslog text varbind value. This is a template field, which means that you can either enter static text (like `syslog message received`) or a template containing variables (like `%1 occurred on %3 for %2`). See the next topic for more information about Template Fields.

Suppress Alarm — Indicates whether or not to suppress the alarm for the resulting event. If you only want events to be created in the Event History but you do not want alarms to also be created, then check this box.

Template Fields

Template fields are associated with specific varbinds. When a syslog message matches an escalation filter, OpenManage Network Manager creates an event and populates its varbinds using the respective templates and the *Message Pattern*.

Templates have numbered variables—`%1`, `%2`, and so on. OpenManage Network Manager resolves such variables with substrings extracted from the original message text. This means it inserts the first pattern retrieved in place of `%1`, inserts the second pattern retrieved for `%2`, and so on. For example: the *Message Template* field contains `%1 occurred on %3 due to %2`, the *Message Pattern* contains the regular expression `(.*): (.*). IP: (.*)` and a syslog message arrives that matches the *Syslog Match Text* with the contents: `Error: out of memory. IP: 192.168.0.1` then the message text varbind on the resulting event resolves to `Error occurred on 192.168.0.1 due to out of memory`. This works on other template fields too, like Category.

OpenManage Network Manager's syslogNotification event also includes a varbind containing the original syslog message. This can be useful if you want the syslogText varbind to be the product of processing but you also want to see the original message.

Message Test

This screen lets you test your message against the pattern and/or template. Click the *Test* button to the right of the top field to activate this testing.

Test Message—Enter a message to test.

Test Message Result—The text extracted for the event as it appears in the template after you click the *Test* button.

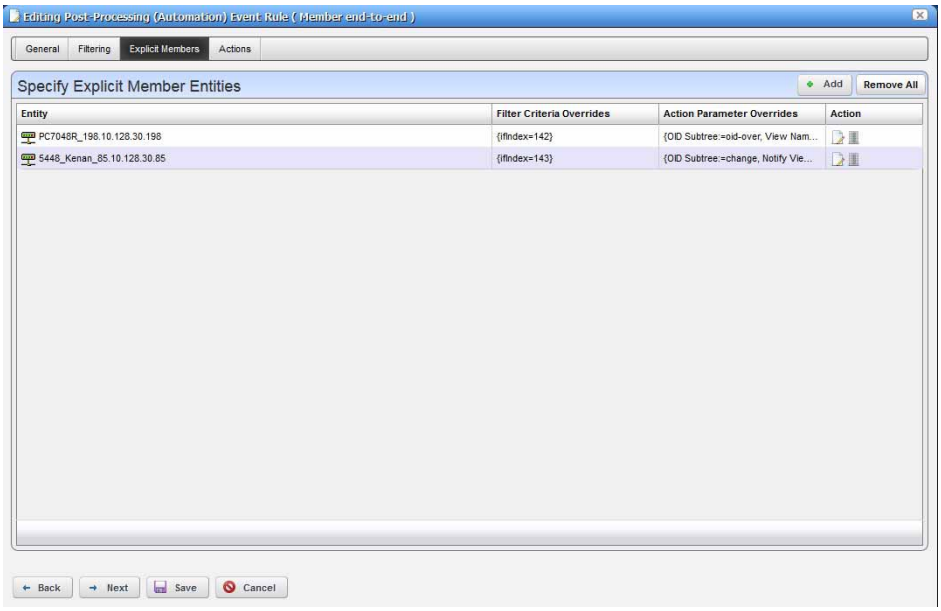
Click *Apply* to accept these escalation criteria, or *Cancel* to abandon them without saving.

NOTE:

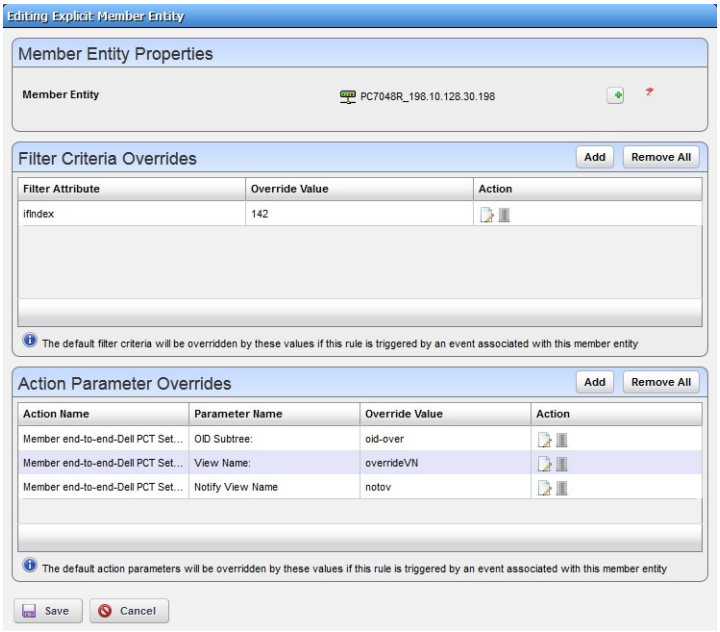
The default behavior of the syslogNotification is Reject rather than Suppress. This means that received syslog messages have to match an escalation filter to become events. Users who want all received syslog messages to become events must override this default setting and change the behavior to either Suppress (which makes only events but no alarms) or Alarm (which makes alarms). Note that this default behavior only affects messages that do not match any escalation filter. Redcell processes those that match an escalation filter just the same regardless of what is the default behavior of syslogNotification.

Explicit Members

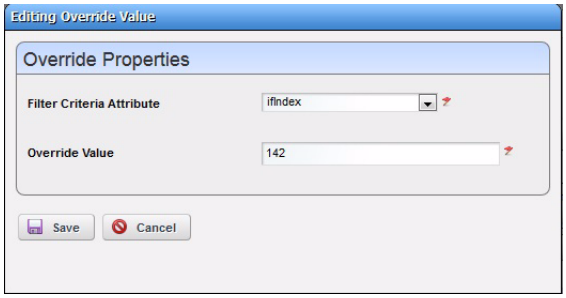
This screen displays the explicit member entities that are associated with this rule. If any explicit members are defined for a rule, then the event must be associated with one of these entities in order for this rule to be triggered. This is a convenient way of defining entity-specific filters for the rule and you can also use this feature to allow the rule to behave differently based on the entity that is associated with the triggering event. Please note that the Explicit Membership box on the *General* tab must be checked in order to enable the buttons on this tab.



If explicit membership is enabled, then you can click *Add* and this displays a screen through which you can select an explicit member entity and optionally configure specific overrides that would be associated with this member.



From the *Editing Explicit Member Entity* popup screen, you can select a **Member Entity** from among different possible entity types including Managed Equipment, among others. You can also specify **Filter Criteria** Overrides, which are the changes to the filter criteria that should be applied when this rule is triggered by an event associated with the Member Entity that was selected. Finally, you can specify **Action Parameter Overrides**, which are changes to the action parameters that should be applied when this rule is triggered by an event associated with the member entity that was selected. If you choose to add an override of either type, a screen will be shown that allows you to specify the attributes that are being overridden along with the override value.

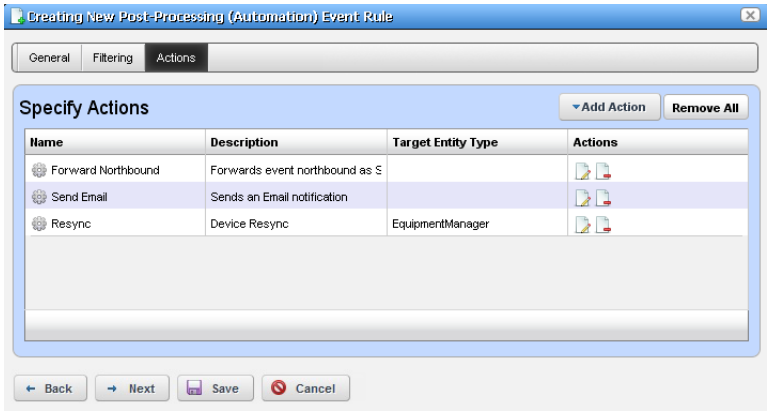


On the *Editing Override Value* screen, if this is a filter criteria override then a drop down list will be shown to select the **Filter Criteria Attribute.** Note that this list will be populated with the filter criteria that this rule is configured with from the *Filtering* tab. If you select an attribute and then enter a value then this value will override the default configured value on the *Filtering* tab if this rule is triggered by an event associated with the configured member. The filter will then be applied with the override values and this rule will only be triggered if these criteria are met.

If this is an action parameter override then drop down lists will be shown to select the action and the action parameter. Note that these lists will be populated with the names of the items in the *Actions* tab and also with the parameters associated with each respective action. If you select an action and an action parameter and then enter a value then this value will override the default configured value on the *Actions* tab if this rule is triggered by an event associated with the configured member. The action will then be executed with the override values.

Actions

This screen catalogs the actions configured for the Automation rule you have configured in previous screens.



Click *Add Action* to create a new action in the editor. The *Actions* column lets you revise (*Edit this entry*) or *Delete* entries in this table. Click *Save* to preserve the action(s) configured here, or *Cancel* to abandon any edits.

Clicking *Add Action* lets you select from the following:

- Action
- Forward Northbound
- Email

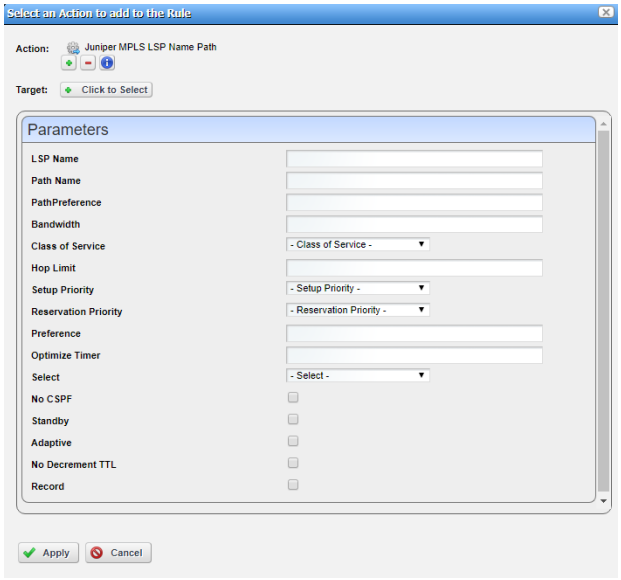
Click *Apply* to accept configured actions, or *Cancel* to abandon their editor and return to this screen.

NOTICE

Actions available here are like those for Discovery Profiles Portlet on page 552. You can also use actions to Execute Proscan. See .

Action

This screen lets you configure an action based on Adaptive CLI actions available in the system. Select an action. To search for an action, specify search criteria and then click Go. The parameters available vary depending on the selected action. Tooltips provide additional information when you hover over a field.



Optionally select the action device target from the list. If you do not specify an explicit target, OpenManage Network Manager uses the default entity for the event as the target.

You can specify parameter variables, dependent on the event, rule, and selected targets specifics. Do this with either NOTIFICATION or VARBIND.

The following are valid attributes to use in a phrase like `[[NOTIFICATION: <attr name>]]`:

- TypeOID
- AlarmOID
- EntityOID
- EquipMgrOID
- DeviceIP
- SourceIP
- EntityName

NOTICE

Consult the relevant portlet to find and verify an OID. For example, the Event Definitions portlet has an OID column, and the varbind OIDs appear in the event editor *Message Template* window.

Correct spelling is mandatory, and these are case sensitive. NOTIFICATION and VARBIND must be all caps, and within double brackets. The colon and space after the key word are required.

OpenManage Network Manager converts anything that conforms to these rules and then passes the converted information into the action before execution. Anything outside the double square brackets passes verbatim.

For example, the string:

```
This is the alarm OID [[NOTIFICATION: AlarmOID]] of notification
   type [[NOTIFICATION: TypeOID]] having variable binding
   [[VARBIND: 1.3.4.5.3]]
```

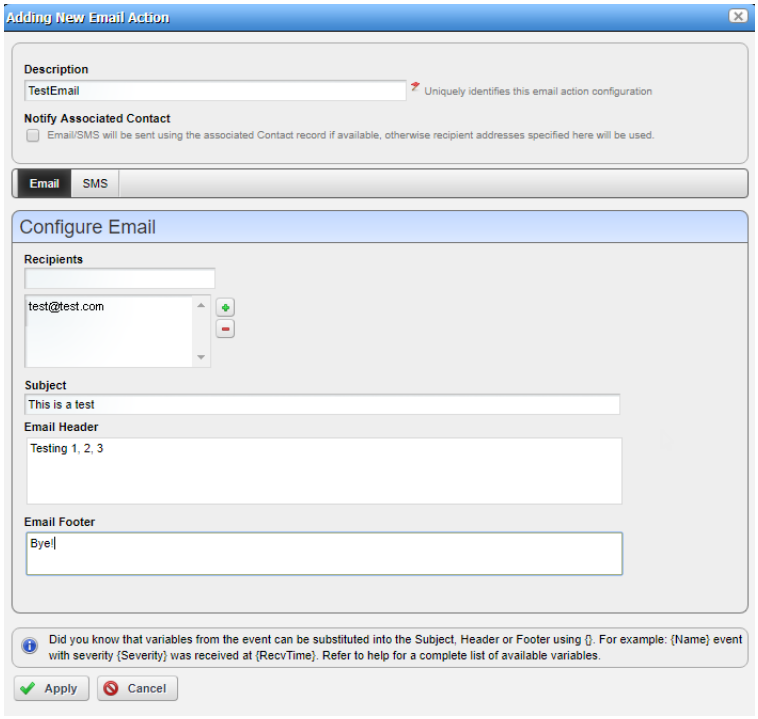
becomes something like...

```
This is the alarm OID 1OiE92tUjl13G03 of notification type
   1.3.6.1.4.1.3477.1.27.20.7 having variable binding 151.
```

Click *Apply* to accept your edits, or *Cancel* to abandon them. For an example, see Extracting Adaptive CLI Attributes from a Syslog Alarm on page 104.

Email

Email actions configure destinations and messages for e-mail and SMS recipients. You can include fields that are part of the event by using the features described in Using Email Action Variables on page 100.



Notice that below the e-mail action Description, you can check to send this mail (and/or SMS) to associated Contacts, if any are available, even if you specify no mail address destination. The SMS tab is similar to the e-mail tab, but limits the number of characters you can enter with a field at its bottom. You must send SMS to the destination phone carrier's e-mail-to-SMS address. For example sending text to 916-555-1212 when Verizon is the carrier means the destination address is 9165551212@vtext.com.

When enabled, notification emails go to the Contact associated with the Managed Equipment for the notification event. For the contact's email address, mail goes to the first specified address from either the *Work Email*, *Home Email* or *Other Email* fields in the Contact editor. SMS messages go

to the *Pager Email* field for the contact. If a Contact was not found or the required addresses are not specified for the Contact, then OpenManage Network Manager uses the Recipient addresses configured in the Email Action.

NOTICE

Programs other than OpenManage Network Manager let you manipulate mail outside the scope of OpenManage Network Manager. For example IFTTT (If This Then That) lets you send SMS in countries whose providers do not provide e-mail equivalents to SMS addressing. You can also use such applications to save mail attachments like reports to Dropbox accounts.

This screen has the following fields:

Recipient —Enter an e-mail address in this field and then click add (+) to add a recipient's address. Click delete (-) to remove selected recipients.

Subject—The e-mail subject.

Email Header/Footer—The e-mail's heading and footing.

SMS Body—The e-mail contents to be sent as text.

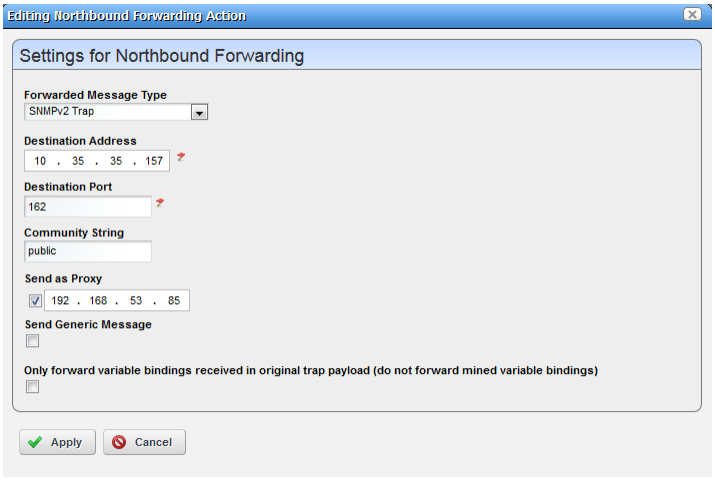
SMS Max Length—The maximum number of characters to send in the SMS. Typically this is 140, but the default is 0, so be sure to set to your carrier's maximum before saving.

Here is what Email looks like when it arrives:

```
Sent: Wednesday, March 02, 2011 2:37 PM
To: techpubs@testsoftware.com
Subject: Web Test
Notification: redcellInventoryAttribChangeNotification
Notification Attributes:
================================
sysUpTime.0                     = 5 hours, 16 mins, 43 secs
snmpTrapOID.0                   = 1.3.6.1.4.1.3477.2.2.1
redcellInventoryAttrName.0      =
   RedCell.Config.EquipmentManager_Notes
redcellInventoryAttrChangedBy.0 = admin
redcellInventoryAttrNewValue.0  = hello
world
severity
auto
redcellInventoryAttrOldValue.0  = hello
world
severity
```

Forward Northbound

When you want to forward a message, such as an SNMP v2 event (trap) to another host, then configure automation in this screen to do that.



Enter the following fields:

Forwarded Message Type — The type of message to forward. This can be an SNMP v2 Trap, a Syslog, or an HTTP REST call. This selection is determined by the type of message the northbound system is expecting. For example, you might have a northbound system that is expecting to collect SNMP traps from OpenManage Network Manager. Some northbound systems are configured to collect Syslog messages and other might be configured to collect HTTP REST calls.

Destination Address—The IP address of the northbound destination.

Destination Port—The port on the northbound destination. Note that this auto-populates with the most common port number based on the selected Forwarded Message Type.

Community String —The SNMP community string for the northbound destination. This is only relevant if the Forwarded Message Type is SNMP Trap.

Username — If the Forwarded Message Type is HTTP REST call, the username is required for authentication.

Password — If the Forwarded Message Type is HTTP REST call, the password is required for authentication.

Send as Proxy—Select this option to send the IP address you specify as the event source. If not selected, the IP address of the mediation server receiving the trap is sent. (See Sending as Proxy on page 97 for more information.)

Send Generic Message —When selected, this sends a generic message, whether this be a trap or a different kind of message. See Forwarding a Generic Message on page 98 for more information.

Only forward variable bindings received in original trap payload (do not forward mined variable bindings) — If selected, only the variable bindings received in the original trap payload is forwarded. If not selected, the mined variable bindings are also forwarded. If the Forwarded Message Type is Syslog, this is irrelevant because Syslog messages do not contain variable bindings.

Event Definition Editor

This editor lets you modify event definitions in the following tabs:

- General
- Message Template
- Correlations
- Extensions

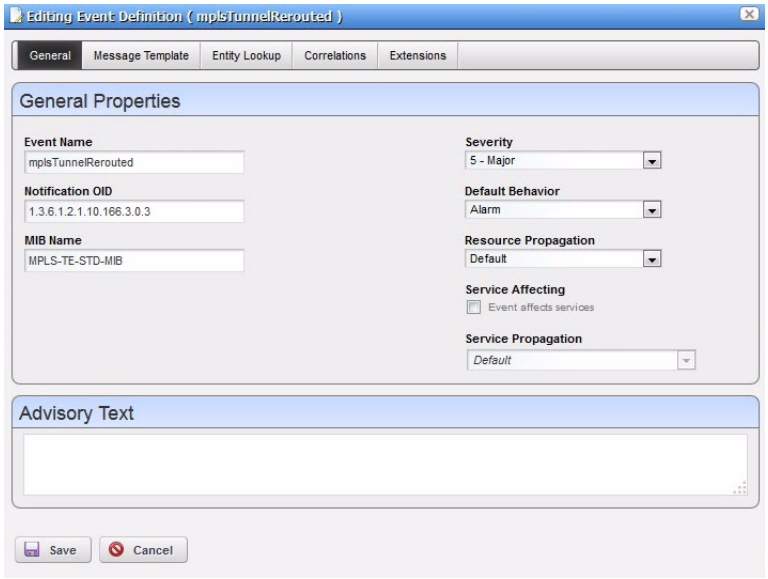
You can also do the following:

- Adding Extended Event Definitions

Click *Save* to preserve any modifications you have made, or *Cancel* to abandon them.

General

This tab manages basics for Event Definitions.



It has the following fields:

Event Name—A text identifier for the event.

Notification OID—The object ID.

MIB Name—The MIB with which this event is associated.

Severity—The severity of any associated alarm. If a new alarm is a clearing severity, then it closes any existing alarm to which it correlates. Otherwise, if a new alarm severity does not match the existing severity then the existing alarm is closed and a new alarm opened for the new severity.

Default Behavior—The options for behavior (*Undefined*, *Alarm*, *Suppress*, *Reject*). *Alarm* means: Process at the mediation server, generate event history and an alarm. *Suppress* means: Process at the mediation server and generate an event (*not* an alarm). *Reject* means: Reject at the mediation server (do not process)

Resource Propagation—The hierarchical resource propagation behavior for any alarm based on this event definition (either *Default*, *Impacts subcomponents*, or *Impacts top level*, or *Impacts Top Level and Subcomponents*). (See also Understanding Alarm Propagation to Services and Customers on page 119 for more about how this impacts services and customers.)

An event definition configures "Resource Propagation" (distinct from "Alarm propagation") based on the event type. Do alarms based on this event definition impact the overall device (*Impacts top level*), subcomponents (*Impacts subcomponents*), both (Impacts Top Level and Subcomponents) or just the correlated inventory entity (*Default*)?

Alarm behavior differs for monitorAttributeTrend alarms when an SNMP Interface monitor targets a Port/Interface rather than targeting a device. If the alarm comes from the former, and its correlation state is not *Top Level Alarm*, only the port appears alarmed, not the device. If the monitor target is the device, however, the device appears as alarmed. If the monitor has Port targets, then you must configure propagation to *Top Level Alarm* to see the device alarmed in, for example, the Visualize My Network topology.

Service Affecting—Check this if the event has an impact on services. Indicates whether the alarm has an impact on services. If this is checked then alarms based on this event definition propagate calculated alarm states across services and customers that depend on the (directly) alarmed resource.

For example: If a resource has a service affecting alarm, then OpenManage Network Manager propagates the severity of this alarm across all associated services and customers. If the resource alarm is "clear" then all services depending on this resource are "clear" too. If the resource alarm is "critical," then all services depending on that resource are "critical" too.

NOTE:

Alarms imported from previous versions appear as not service affecting, regardless of severity.

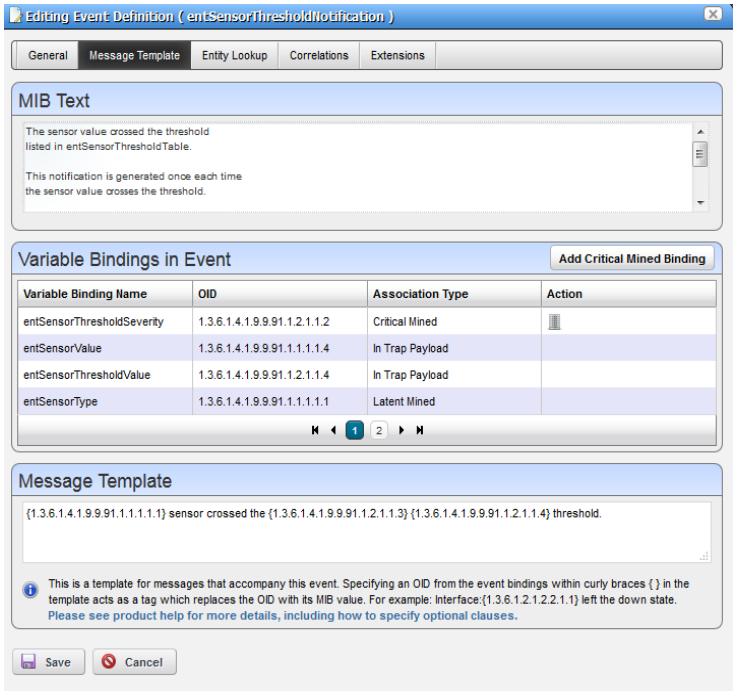
For more about propagation, see Understanding Alarm Propagation to Services and Customers on page 119.

Service Propagation — This only affects alarm propagation if Service Affecting is true for the event definition. This is like *Resource Propagation*, but controls only whether alarms affect services associated with entities hierarchically related to the alarmed entity. For example, if a port alarm is created and its event definition specifies that the Service Propagation is Impacts Subcomponents then the alarm propagates only to the services associated with this port's interfaces. This does not affect the services associated with the top-level device.

Advisory Text—The *Advisory Text* appears with the event. Configure it in the text box here.

Message Template

The Mwssage Template panel lets you view or alter MIB Text, Bindings and the Message Template for the selected event.



This contains three sections:

MIB Text—A read-only reminder of the MIB contents for this OID.

Variable Bindings in Event — Lists the variable bindings that are expected to be in events based on this definition. This displays the varbind contents of the event, matching the *Variable Binding Name*, *OID* (object identifier), and the association type. There are three ways that bindings are associated to event definitions:

- **In Trap Payload** means that the association is determined by the MIB and thus it being mentioned here is read-only.
- **Critical Mined** means that the binding needs to be mined from the device that emitted the trap so that the event is augmented to have this additional information available for the message template, correlation, entity lookup, extensions, or filtering of event processing rules.
- **Latent Mined** means that the bindings are mined only during alarm correlation. This h is too late for such bindings to be available for certain features, such as entity lookup and extensions.

Click the *Add Critical Mined Binding* button to display a list of variable binding definitions from which to select. Critical mined bindings are configured using this option. Latent mined bindings are configured from the variable binding definition level. See Variable Binding Definitions on page 635.

Message Template—A template for messages that accompany this event. Specifying an OID within the curly braces {} in the template acts as a tag which replaces the OID with its MIB value. For example: Interface: {1.3.6.1.2.1.2.2.1.1} left the down state.

You can also add optional messages surrounded by double brackets [[ ]]. if the event definition has the message “aindex: {1.2.3}[[, bindex: {1.2.4}]]” and {1.2.3} is defined as say “1” but {1.2.4} is not defined then this resolves to “aindex: 1". If they are both defined (say {1.2.4} is “2”) then this resolves to “aindex: 1, bindex: 2"

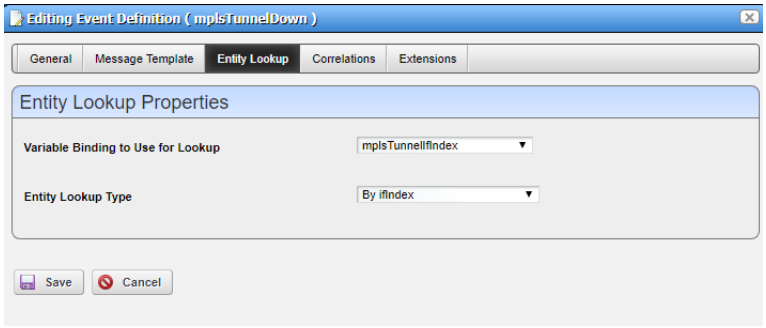
If a message template exists for an existing, correlated alarm and the generated text does not match the original alarm, then OpenManage Network Manager closes the existing alarm, and generates a new one. Leaving this blank transmits the original message.

NOTICE

Putting an OID in curly brackets amounts to a tag replaced by the MIB text for that OID. Look for OIDs and messages in the MIB browser (as described in MIB Browser Tool on page 550).

Entity Lookup

This screen lets you configure how events based on this definition will be associated to entities. By rule, the Equipment attribute of any event will be determined by the source IP address of the original message (trap, syslog, etc.) By default, the Entity attribute will be the same as the Equipment, but there might be information in the variable bindings of the trap through with the event can be resolved to a subcomponent (Port, Interface, etc.)

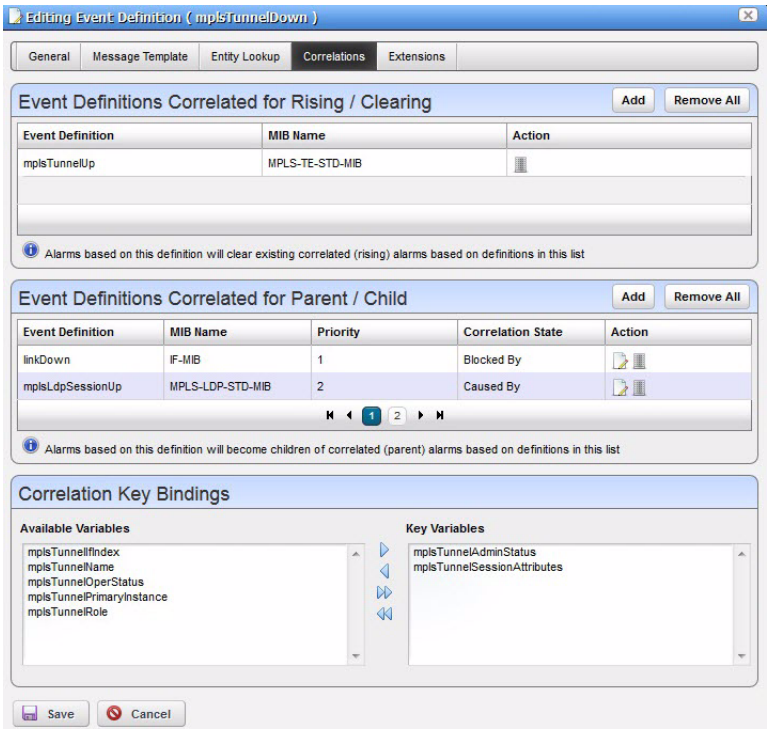


Variable Binding to Use for Lookup — Indicates the variable binding that should be used for the entity lookup. This drop down list includes all bindings that are expected to be in the trap payload and also those that are critical mined. Latent mined bindings cannot be used for this purpose.

Entity Lookup Type — IndIndicates the algorithm that should be used to lookup the entity. For example, if the variable binding to use for lookup contains an ifIndex then you should select By ifIndex. It might also be that it instead contains the physical index, in which case there are two options, either By Physical Index (simple) to simply lookup the entity by this given physical index and associate to that entity directly, or By Physical Index (find parent) to instead use the physical index to find the hierarchical parent. This is useful when a vital component of a device, like a power supply or a fan, has sensors attached. Traps coming from this device contain the physical index of the sensor rather than the vital component being monitored. This lookup type lets you associate alarms with the vital components so you can ensure these components are functioning optimally.

Correlations

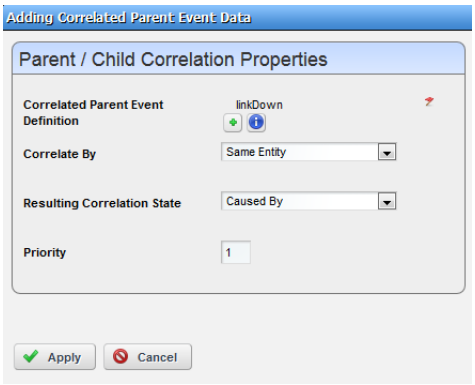
This screen lets you configure different forms of correlation for the event definition including Raising / Clearing Correlated Events, Parent / Child Correlated Events, and Correlation Key Bindings, the latter of which is essential for event to alarm correlation.



The *Event Definitions Correlated Eventsfor Raising / Clearing* panel lets you control what type of events will automatically clear the correlated alarms that are based on this definition. Within this panel, click *Add* to display a selector (with filter) to find events definitions to correlate with the one you are editing. What this means is that if there is an existing open alarm based on this definition (we can call it a raised alarm) and then subsequently another alarm is created that is correlated to the raised one, it will cause the raised alarm to be cleared (it will no longer be open). Note that this will only work if the definition you are editing has the severity of cleared and the definition in the list has a severity other than cleared. For example, link down and link up event definitions are correlated as raising / clearing, and thus all events and alarms based on these definitions will inherit these correlations. So consider that a link down event is received that creates a raised alarm and then subsequently a link up event is created. The link up would then correlate to and clear the link down alarm.

The *Event Definitions Correlated for Parent / Child* panel lets you control what type of alarms will automatically correlate as parent / child relationships that indicate that one alarm caused the other or that one alarm blocks progress on the other. What this means is that an open alarm based on the definition you are editing will form a parent / child correlation to another open alarm based on a definition in this list. Note that alarms based on the definition you are editing will become correlated children of alarms based on definitions in the list (the later will become correlated parents). For example, when new alarms are created that are based on this definition, OpenManage Network Manager will try to find a correlated match between each new alarm and other existing open alarms, and it does this based on the entries in this list. If it finds a match, it will correlate the parent alarm to the child alarm.

Within this panel, click *Add* to display a popup panel through which you can select an event definition to correlate with the one you are editing.



The following fields show on this screen:

Correlated Parent Event Definition — Displays a selector (with filter) to find the event definition to correlate to the one that you are editing. Alarms based on the definition you select will be correlated parents of alarms based on the definition that you are editing.

Correlated By — This is the algorithm that is used to determine if there is a correlated match between any potential parent and child alarms. Currently the only option is Same Entity, meaning that the two alarms must be associated with the same entity in order to be correlated in this way.

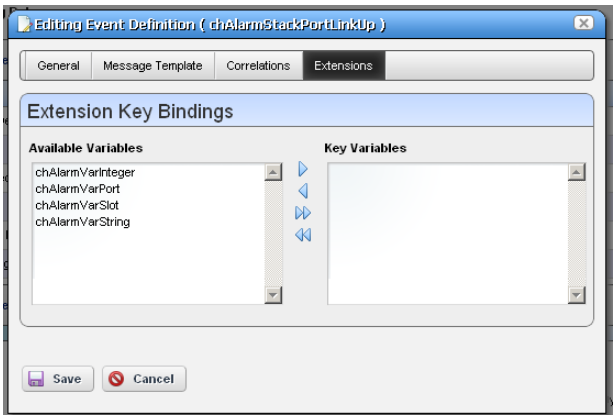
Resulting Correlation State — This indicates the type of parent / child correlation that should be created. Caused By indicates that the parent alarm caused the child alarm to be created and Blocked By indicates that the parent alarm is blocking progress on the child alarm. The most significant difference in terms of how such correlations are processed occurs when the parent alarm is cleared. In such scenarios, caused by children will be cleared automatically when the parent is cleared, whereas blocked by children will simply be unblocked when the parent is cleared.

Priority — Indicates the priority that this entry should have in relation to the other entries in the list. If there are multiple entries in this list, then OpenManage Network Manager will first try to find correlated matches based on the entry with priority 1 and then if there are no matches it will try to do so based the entry that is priority 2, and so on.

In Correlation Key Bindings, use the right/left arrows to select *Key Variables* from *Available Variables*. The variables considered keys for event to alarm correlation are the key bindings for the target alarm in the correlation process. This means that if event A is defined to include event B as a correlated event, comparison of the key bindings defined for event B is also considered when comparing a new alarm for event A to an existing alarm for event B.

Extensions

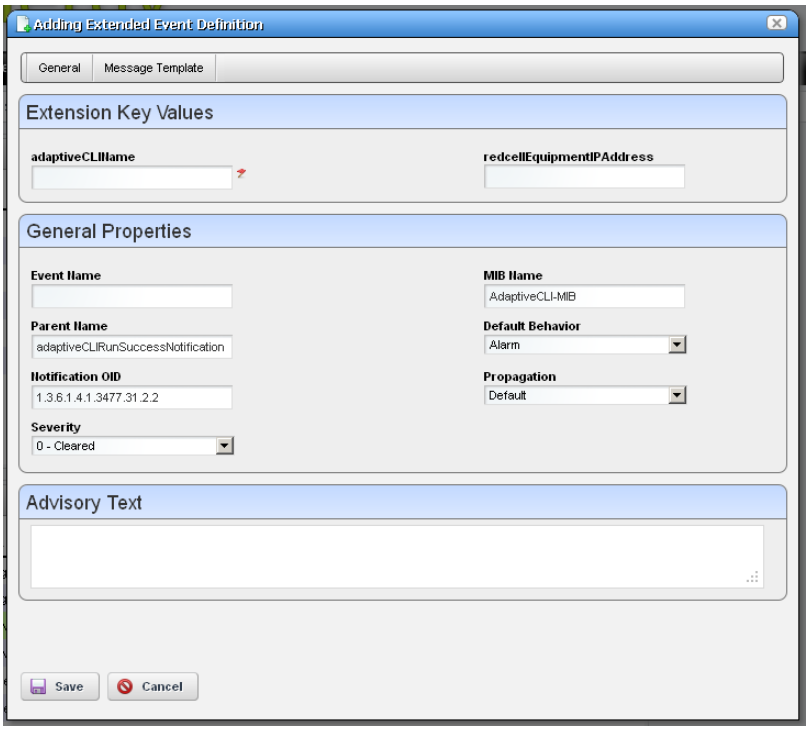
ThisSTART panel lets you configure Extension Key Bindings. Extensions enable Adding Extended Event Definitions.



In Extension Key Bindings, use the right/left arrows to select *Key Variables* from *Available Variables*. For example, if a device generates one type of trap, but has three key variables (alarmID, state, and severity), you may extend the event definition based on state. One derived definition for the “alarm” state and another for the “clear” state. You probably would extend based on state and severity to define a clearing definition for all events where state is “clear” and then derive a specific “alarm” event for each severity as defined by the vendor.

Adding Extended Event Definitions

The menu item for this screen can appear when you right-click an extendable event (one that has one or more Extensions). For an implemented example, see Extending Event Definitions on page 114.



The Extended Event Definitions editor screen has the following fields:

Extension Key Values

The fields that appear in this panel are those configured in Extensions.

General Properties

Event Name—An identifier for the Extended Event. This field is editable, but if left blank the system creates a name based on the name of the parent event definition and the key bindings entered here.

MIB Name—A MIB identifier for the Extended Event

Parent Name—An identifier for the parent of the Extended Event

Notification OID—As with parent event definitions, this is the object ID. OpenManage Network Manager automatically generates this based on the Notification OID of the parent and key binding values entered. For example, if the parent event definition has a Notification OID of "1.2.3.4" and the key binding values of the extended definition are 5 and 6 (the parent must have previously been configured to have two extension bindings available) then the resulting Notification OID for this new extended event definition will be "1.2.3.4::5:6".

The remaining fields are as described in the Event Definition Editor General screen. The Message Template tab is as described in Message Template on page 500, only this message template is for the configured extended event definition.

Click *Save* to create or re-configure an extended event, or *Cancel* to abandon your edits. See Extending Event Definitions on page 114 for detailed steps.

Container Manager Portlet

Container manager lets you create, edit and delete Container tree models displayed in Container View Portlets (described in the next section). These containers filter what appears in other portlets on the page with the Container View Portlet portlet.

The relationship to users and devices appears in Container Manager Expanded.

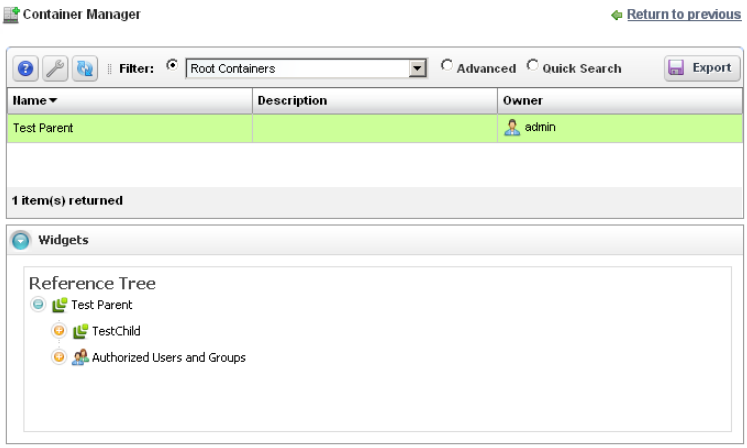
Right-click to select from a menu with *New, Edit* and *Delete,* and *Refresh Members / Alarm State. Refreshing* re-queries the database for members fitting the dynamic filter, or for new alarms for members. Selecting *New,* or *Edit* displays the Container Editor.

You can also *Tag* containers so Map views show containers. See *Tag on page 512* for more about how that works.

Access this portlet by selecting the Alarms > Alarms by Container page.

Container Manager Expanded

The expanded view displays the same information as the summary view, but displays the selected container's authorized users, creator, owner, and membership in the Reference Tree snap panel.



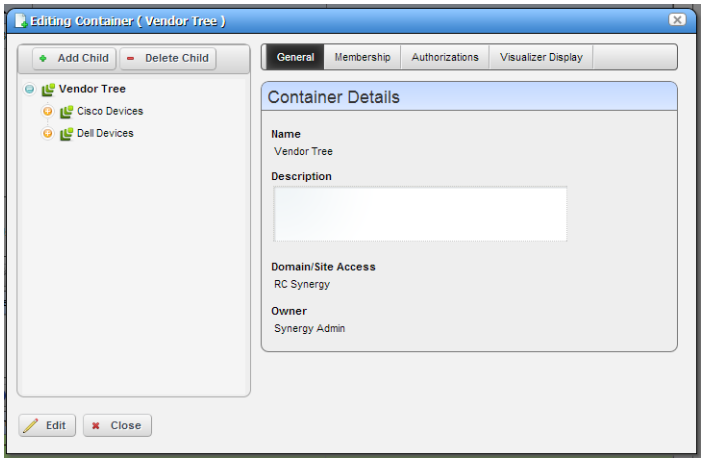
Menu items and columns are like those for the summary portlet.

Multitenancy and Containers

If you have the multitenancy option installed, you can limit a container's visibility to a tenant site, or to the entire system. You can also import containers to target multitenant domains with a command line importer. The command is `importcontainers` and is in the `owareapps/redcell/bin directory.` This command takes the import file name an argument. The required domains should be available in the OpenManage Network Manager system before import occurs. Example XML files (with the `<customer>` tag for domains) are in `owareapps\redcell\db.`

Container Editor

This editor lets you create and manage containers. You can also associate user authorizations with container models to specify which groups or users have access to contained items.



In this editor, a tree panel on the left lets you build and navigate the container tree. Click *Add Child* (or *Delete Child*) to create (or remove) a node to / from the node you have selected in the tree. Clicking a node in the tree displays the tabbed panel on the right where you can edit it.

The *Container Details* panel has the following tabs:

- General
- Membership
- Authorizations
- Visualizer Display

Click the labels at the top of the screen to access these. Alarm states and severities are recalculated and propagated for containers as they are for Visualize My Network on page 516.

General

This panel has the following fields:

Name—The container identifier.

Description—A text description of the container.

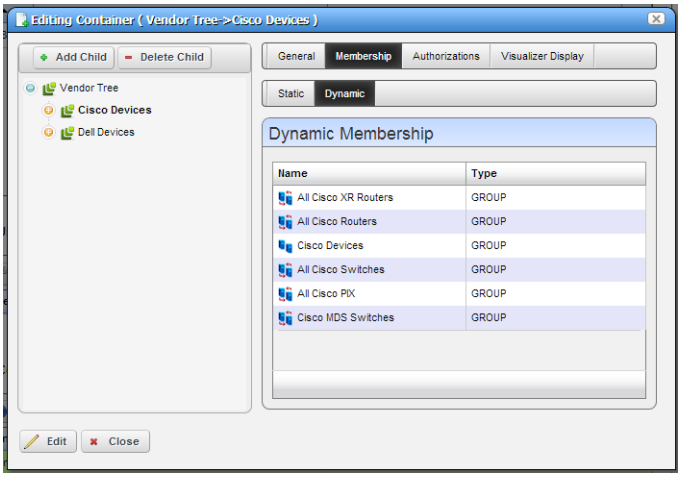
Domain/Site Access—If you have the Multitenancy option installed, to expose a container or sub-container within a site the container must specify that site. You can confine a container's contents to what is visible on a single site. All container contents are visible for the master site.

Owner—Select an owner for the container. The owner of a container can also change the ownership of the container

Update View Authorizations—Clicking the link here automatically includes the creating user in those authorized to view the container. See Authorizations below for more about them.

Membership

Container membership defines the inventory items that are in a container. You can select either a *Static* membership, which cannot change, or a *Dynamic* one, based on a filter or existing group(s). When OpenManage Network Manager evaluates the filter it adds the resulting items as members in the container.



The sub-tabs at the top of the screen let you edit these types. You can add individual items with the *Static* tab, or the results of a *Dynamic* filter with that tab. See Managed Resource Groups Portlet on page 637 for more about the specifics of editing these dynamic groups.

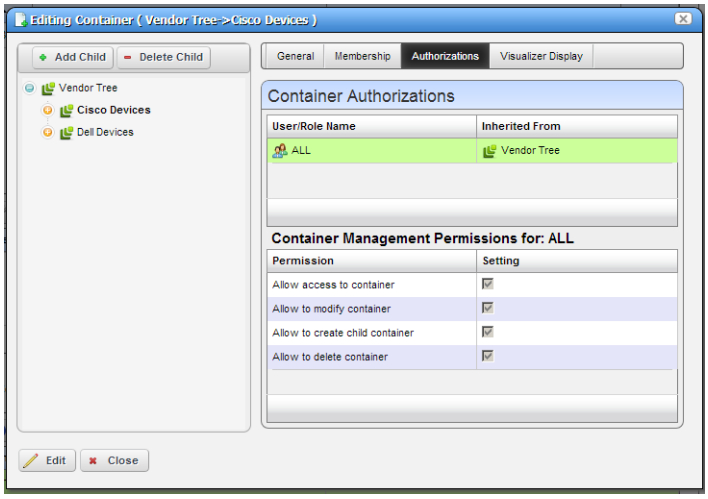
When you add an item or filter to your container, notice that the subsequent screen contains a pick list *Select an entity of the following type*. The contents of that list can contain several types of managed objects, including Contact, Equipment and Subcomponent, Interface, Location, Managed Equipment, Port, and Vendor. Select the type appropriate for your container.

Click *Save* to preserve the membership you have configured. If you *Group By Entity Type* (at the bottom of the screen) rather than *None*, the list of devices appears in a tree, with each node as an entity type. Click the plus (+) to the left of the entity label to expand the tree.

Authorizations

This tab configures user or role access to the container you are editing. By default, no authorization exists to see a container or its contents, so you must permit specified users and roles to have access before any containers or their contents are visible in the Container View Portlet portlet.

Click *Add User* or *Add Role* to select the users or groups with permission to access the container you are configuring. By default containers are accessible to everyone.



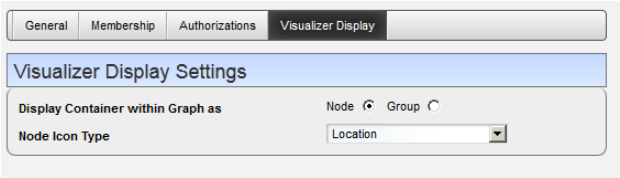
Each entry in the Container Authorizations list specifies the name of the user or role, and whether the entry is inherited or not. A child container by default inherits the authorizations from parent hierarchy, no explicit authorizations for child containers are necessary. Edit any authorizations in the parent.

When editing a child container, click a listed authorized user or role and its permissions appear in the panel at the bottom of this screen.

Clicking *Save* preserves any alterations you have made. Confirm the container is configured as you like by examining it in a Container View Portlet portlet.

Visualizer Display

This tab configures how the container appears in the Visualize My Network portlet.



Selected containers' labels appear in the Visualizer's title bar. Configure the following display settings in this panel:

Display Container within Graph as—Select either *Node* or *Group*.

Node Icon Type—This appears if you select *Node*. Use the pick list to select among the various icon types as is appropriate for your container.

Group Style—Select either *Default (Rectangle Shaded Group)* or *Cloud (Cloud Background Image)*. The group is like the Expand Grouped capability described in *Configuring Views on page 523*. The Cloud is a cloud icon like the one you can add to views as described in *Visualize Portlet* on page 517.

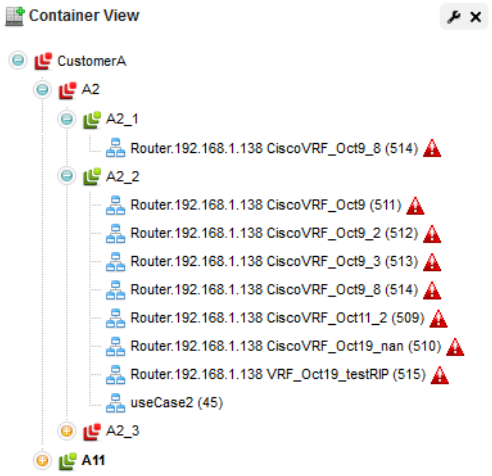
Display Container Name within Group—This appears if you select *Group*. Check it to display the container name as a label within the group.

Container View Portlet

This (non-instanceable) container portlet displays configured containers authorized for the logged-in user, in the color of the most severe alarm for equipment within that container. Because it is non-instanceable, only one can appear on a page.

Filter what appears on a page using the Container View portlet. Select a container, and the rest of the portlets on that page filter their data reporting to reflect that container's contents. The only caveat to this type of filtering is that you can add only one Container View portlet to a page.

Access this page by selecting the Alarms > Alarms by Container page.



Expand the container tree by clicking the plus to each container's left. Container contents sort alphabetically, and alarms appear to the right of equipment displayed.

The container selected acts as a filter for a screen's other OpenManage Network Manager portlets. If you select "Folsom" as a location in the container portlet, then only items related to Folsom devices appear in the other portlets on the page. If you select a parent container, that expands the selection to include all child containers' selections. It does not, however select everything. You can configure containers in Container Editor, described in the next section. You may have to wait a few moments to see a container's contents accurately.

Portlets that respond to Container or Map Context "filtering" include the following: Audit Trail, Event History, Locations, Vendors, Contacts, Managed Resources, Ports, Authentications, Discovery Profiles, Monitors. If you have no containers configured, the other portlets appear empty when Container View is on the same page.

See General > Entity Change Settings on page 687 for the way to set the summary portlet refresh interval. The default is 40 seconds. If this portlet is in expanded mode, refresh does not occur automatically, but you can refresh it manually.

NOTICE

If a container displays unexpected results or no members at all, right-click it to refresh its membership or alarm severity / state. Remember also that the visible changes may take a moment to appear.

Right-clicking a container displays the following menu items:

Refresh Members—Re-query the database to populate any dynamic filter that is part of the container.

Details—Opens a details panel with a list of the container's contents (*Members*) as well as container members' *Alarms* (Alarms and Event History) and *History* (Audit trails and Configurations).

Refresh Alarm State—Re-query the database to update the container's alarm state based on its contents.

Edit Resources—Open an editor screen for the container that lets you change common attributes within it.

Visualize—Display a container in the Visualize screen where you can drill in to see its contents (see Visualize My Network on page 516).

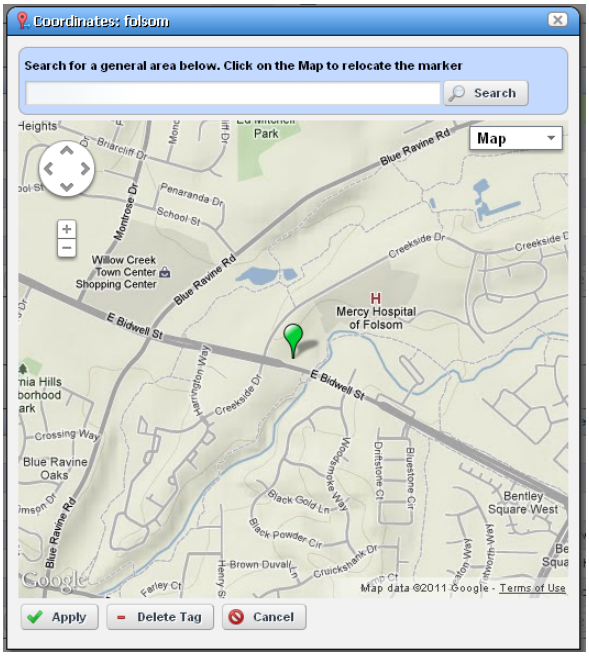
Tag—Enter map location coordinates for the container. See below for more.

Container View in Tenant Sites

Within a Multitenant environment, only containers configured to appear in tenant sites appear there. If that container contains equipment only visible on the master site, those devices will appear below the container node, but will have no impact in filtering other portlets, like Alarms, for example.

Tag

When creating a container or customer tag, OpenManage Network Manager automatically selects the latitude and longitude of the address entered for a location. Tag a container by right-clicking it from the Container Manager Portlet on page 506.



You can also enter the address in the Search field, or click and drag the marker that appears on this screen. Click *Apply* to accept the re-location. A *Delete Tag* button appears when you have created a tag, and lets you remove it. *Cancel* closes the screen.

NOTE:

You can zoom in or out on the displayed map with the + and - buttons in the upper left corner of this screen.

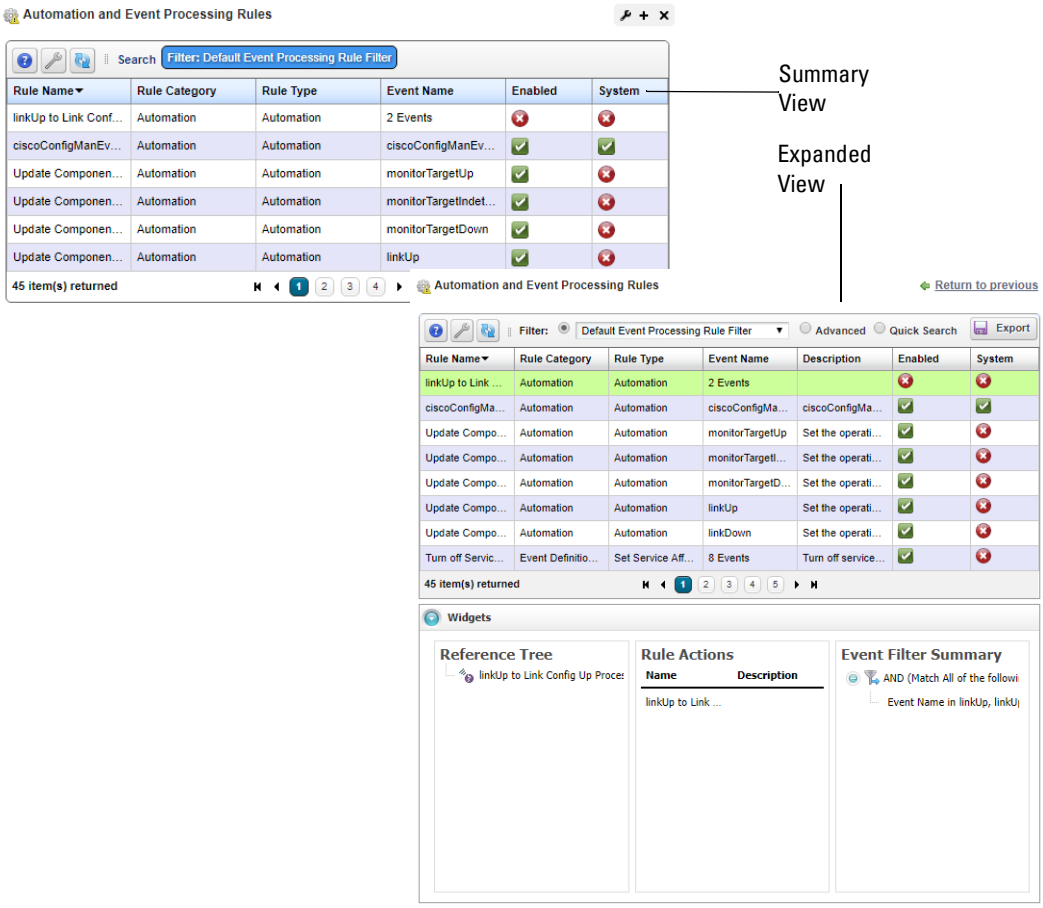
Automation and Event Processing Rules

Automation and Event Processing Rules

Use the Automation and Event Processing Rules portlet to configure and maintain event processing and automation rules.You can create custom multitenant domains and event processing rules (EPRs) within any Multitenant site. Aside from the filter criteria, which EPR applies depends on the EPR's Domain ID compared to the target entity's notification Domain ID. All EPRs with the root site's Domain ID apply to all arriving events. EPRs with another Domain ID only apply to events for entities that have been assigned the same Domain ID.

This portlet is intended for users who are interested in configuring and maintaining event processing and automation rules. For steps to create these rules, see Creating Event Processing Rules on page 95.

Access this portlet by selecting Alarms > Automation from the navigation bar. This portlet has both a summary view and an expanded view. Each view could display different columns and has the same pop-up menu options available.



Columns

Other than the general navigation and configuration options, the Automation and Event Processing Rules portlets (summary and expanded views) include the following columns. The columns displayed by default are noted.

You can view the value for most of the hidden columns by clicking the Settings tool, selecting the columns tab, clicking Show for the appropriate column, and then applying the change.

Column	Description
Rule Name	A descriptive name given to the rule. This field displays on the summary and expanded views by default.
Rule Category	The stage in the event and/or alarm life cycle that the rule is triggered. For example: • Protocol Translation rules trigger early in the life cycle when non-SNMP messages, such as Syslog are received. • Stream Based Correlation rules also trigger early in the life cycle to minimize the event processing load on the application server and to improve throughput. • Event Definition Override rules trigger after the aforementioned rule categories, but prior to alarm correlation. • Automation rules trigger a little later in the life cycle so that the results from the execution of those rules are taken into account during automation. This field displays on the summary and expanded views by default.
Rule Type	Text that indicates what the rule does. For example, there are several rule types within the Event Definition Override category that change specific event attributes to override default values otherwise inherited from the event definition. To consider a specific example of this, you can make an Event Definition Override Event Processing Rule that sets an event as service-affecting. These rules override the default service affecting field that would otherwise be entirely determined by the event definition (as determined by the notification type). **Note:** The installation provides some seeded event processing rules. You can edit some seeded rules, others you cannot edit. If you edit a system seeded rule and want to restore the default settings, you need to delete the rule from the portlet and then enter `ocpinstall -s` from an oware command line to re-seed the database. This field displays on the summary and expanded views by default.
Event Name	The event associated with the rule. This field displays on the summary and expanded views by default.
Enabled	An indicator that the rule is enabled (checkmark) or not (X). This field displays on the summary and expanded views by default.
System	An indicator that the rule is a system rule (checkmark) or a non-system (user-defined) rule (X). This field displays on the summary and expanded views by default.
Description	Text describing the rule in more detail. This field displays on the expanded view by default.
Widget	Additional information about the selected rule, such as: • **Reference Tree** shows the connection between the rule and its event. • **Rule Actions** list any configured actions associated with the rule. • **Event Filter Summary** shows configured filters for the selected rule. The Widgets field is available **only** from the expanded view.
Component	The component the rule accesses, such as Extreme Networks device driver.

Column	Description
Domain ID	The identifier for the resource domain.
Icon	The icon that represents this resource.
Valid	An indicator that the rule is valid (checkmark) or not (X).

Pop-Up Menu

The Automation and Event Processing Rules pop-up menu provides access to the following options. Right-click a row to access these options.

Menu Option	Description
New	Provides access to the following menu options: • **Protocol Translation** displays the Syslog Escalation option. Select this option to open the Creating New Syslog Escalation Rule window and define a syslog escalation rule. • **Stream Based Correlation** displays the Frequency Threshold and State Flutter. options. Select the event processing rule type to open the Creating New *eventType* Event Processing Rule window and define a new event processing rule. • **Event Definition Override** displays the Reject Event, Suppress Alarm, Set Severity, Set Service Affecting, and Device Access options. Select the event processing rule type to open the Creating New *eventType* Event Processing Rule window and define a new event processing rule. • **Automation** opens the Creating New Automation Event Processing Rule window, where you define an automation processing rule.
Edit	Opens the Editing Automation Event Processing Rule window, where you can view the rule details or edit the rule if it is not read-only.
Copy	Creates a new rule derived from the selected rule with some changes to the properties, filtering, members, or actions. **Note:** The OpenManage Network Manager system generates a new name, such as CopyOfUpdate Component State. You must change that name before you save the event processing rule.
Audit	Opens the Audit Trail Viewer window, which lists existing audit records and jobs for the selected record.
Delete	Removes the selected rule.
Import/Export	Provides the following actions when available for the selected rule: • Import retrieves a file containing XML compliance descriptions. Some imports can come from a URL. • Export Selection exports the selected description to an XML file. • Export All exports all descriptions to an XML file. Click Download Export File to specify where to save the file. The Import/Export option is useful as a backup or to share descriptors with other projects. You must import data into the correct portlet. For example, you cannot import event data into the Actions portlet. If one type of data depends on another, you must import the other data before importing the data that depends on it.
Share with User	Opens the Share with User window where you select the colleague you want to share the selected rules with and then type your message.

Network Management Page

Network Status Dashboard Portlet

The following portlets are displayed when you select the Network Management > Network View menu option.

Virtualize My Network Portlet

Links Portlet

The following portlets are displayed when you select the Network Management > Traffic Flow menu option.

Traffic Flow Applications Portlet

Traffic Flow Endpoints Portlet

Traffic Flow Exporters by Subcomponent

Traffic Flow Exporters by Managed Equipment Portlet

Traffic Flow Conversations Portlet

Traffic Flow Protocols Portlet

Traffic Flow Senders Portlet

Traffic Flow Receivers Portlet

Traffic Flow Autonomous Systems Portlet

Visualize My Network

The Visualize My Network portlet displays discovered devices, mapping them in relationship to each other. It also lets you store and retrieve views you have arranged, as well as configure the default view (see View on page 521 for more about these capabilities).

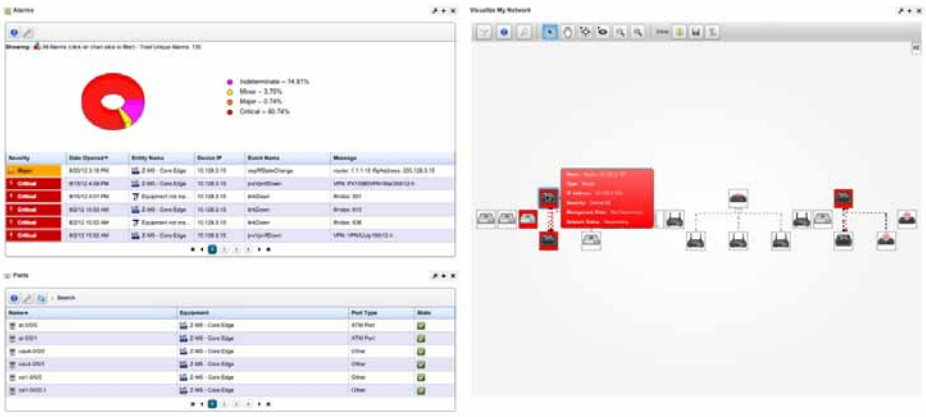
See General > Entity Change Settings on page 687 for the way to set the summary portlet refresh interval. The default is 40 seconds.

The color displayed in these topologies indicates the alarm severity of the node or link ("edge") only. No color or icon indicates a device's network status or availability, although hovering the cursor over a node displays that information.

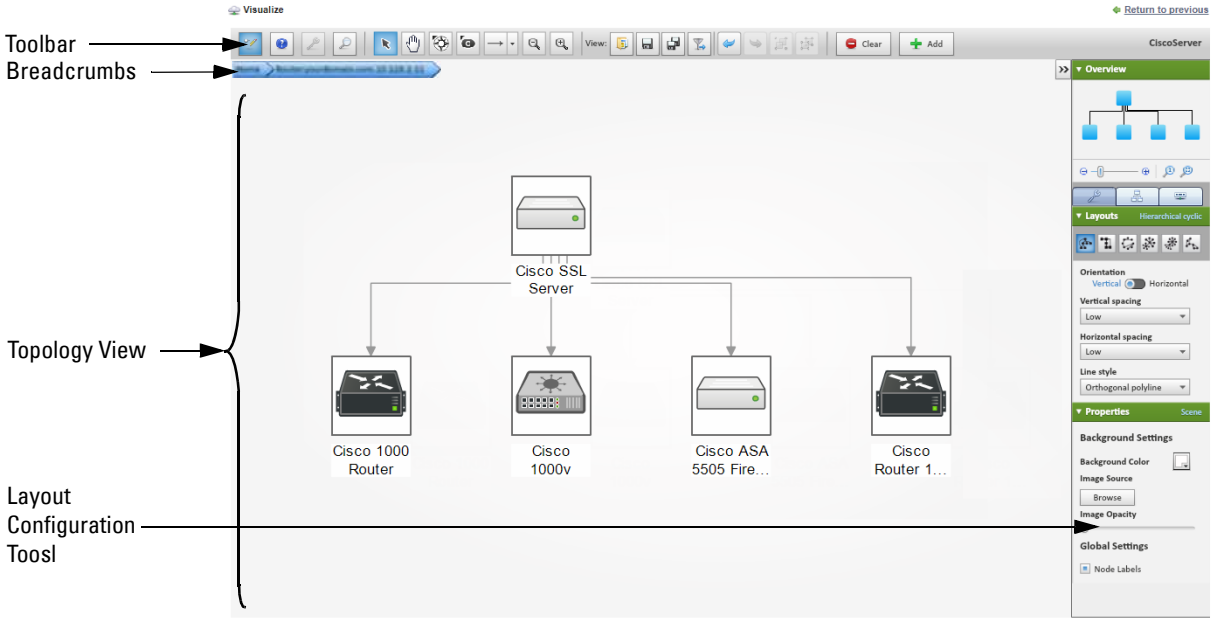
NOTICE

You can increase or decrease the size of icons in the Equipment Editor. Right-click a device in the Managed Resources portlet, and select *Edit*. In the Extended Details panel, select *Settings* and a *Topology Icon Size* pick list appears as one option to configure.

Visualize can act like a filter, too. Portlets like Alarms and Ports respond to clicking a node in Visualize, displaying information relevant to only that node.



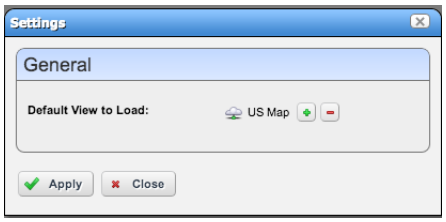
Visualize Portlet

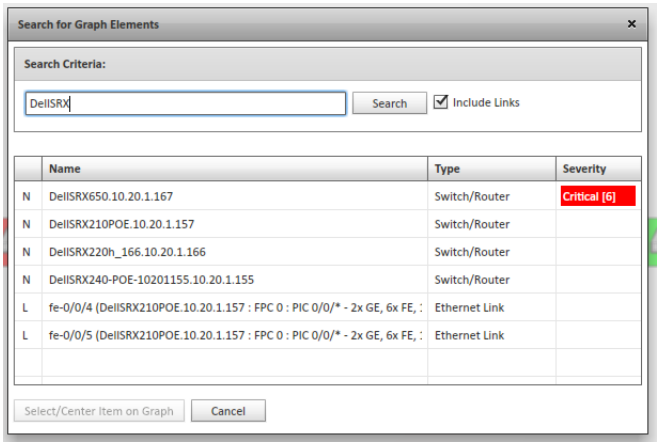


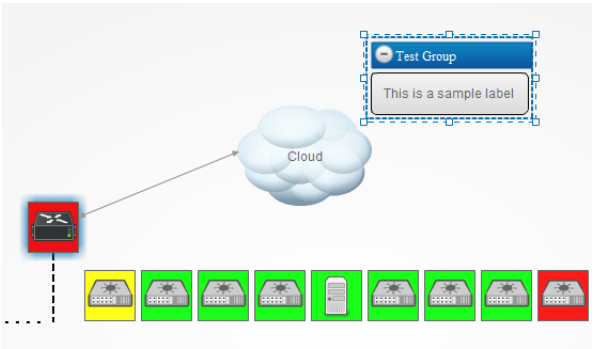
Tools

A Visualize portlet toolbar helps navigate through the topology, load a view, save a view,...

When you click the Toggle Design Mode tool, several additional tools appear that let you manipulate the topology view.

Tool	Description
	Toggle Design Mode (Ctrl+D) shows and hides the design tools, such as the line draw, undo/redo, group/ungroup, and so on. Click this to turn on the design tools, such as line draw, edge filtering, undo/redo, and so on. You can configure users' permissions for Design Mode in *Control Panel* > *Permissions manager*. To disable Design mode, uncheck Visualizer permission both ADD and DELETE for all assigned roles (typically these include User, Power User, and sometimes Administrator). To enable Design Mode check Visualizer permission ADD and DELETE for roles (typically for the Administrator role). To give other-than-administrator users no Design Mode permission, uncheck ADD and DELETE for User and Power User assigned roles.
	Help Click this to turn access the online help for this screen.
	Default Click the wrench icon to configure the default view. If the Visualizer Portlet is on a page not driven by another Context—for example, Containers—and you have write permission for Visualizer, then this icon appears. Clicking this lets you associate the Visualizer portlet on the current page to a selected view. To return to the default  network view click the red minus (-) button in the settings. Any view change requires a page refresh after applying the revised setting.

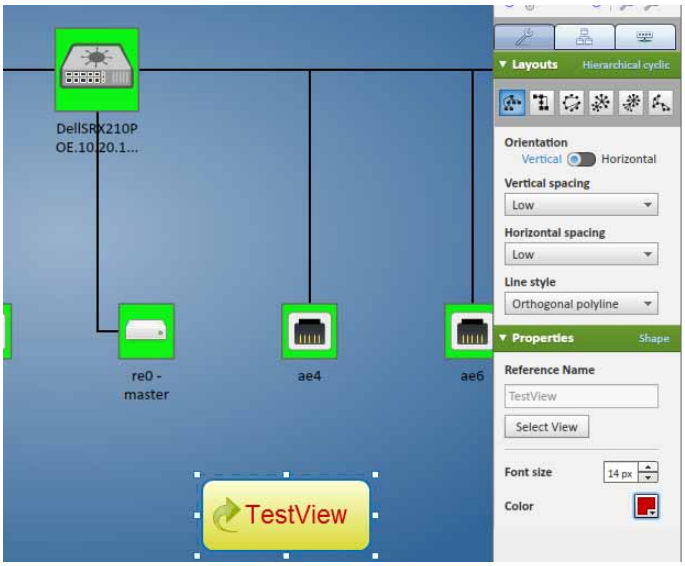
Tool	Description
	Search Node Elements within this Graph (Ctrl+S) Search for a particular node. This opens a screen displaying the search results, name, type of node and the node's alarm severity. Click Select / Center Item on Graph to select a listed item.  **Note:** Search also finds links or "edges" between devices, and saving a view preserves displayed links' appearance.
	**Selection Tool** The cursor selects nodes. Click and drag around nodes to select several.
	**Pan Tool** The hand moves the background.
	**Shortest Path Tool** Click two nodes to highlight the shortest path between them. This simple tool looks for the shortest set of lines, and does not take into account factors like route cost, bandwidth, link status, and so on.
	**Bifocal Effect** Move the cursor to magnify nodes under it. Handy in a crowded view.
	Line Draw Click to select the type of line to draw, then shift+click two icons onscreen to draw the line. hidden with other view tools
	**Zoom Out** These magnifying glass icons change the magnification for the view.
	Zoom In
	Load a View opens a saved view.
	Delete and Reset Factory View tool

Tool	Description
	Save this View tool saves the current. Views include visible nodes and links, but you cannot save the location of these nodes. (See Map Context on page 662 for a possible alternative.)
	**Edge Filtering** tool opens the Edge Filtering window, where you select whether to enable edge filtering and then which links appear in the topology. By default, edge filtering **is not** enabled and all links are selected.
	**Undo** tool reverses the last action.
	**Redo** tool puts the last action back.
	**Group** tool puts the selected objects, lines, and labels together allowing you to move the in tandem. Ctrl+click to select multiple objects. These two icons group or ungroup selected icons labels and lines together so you can move them in tandem. Ctrl+click to multi-select icons. When you create a group, the Properties panel provides additional configuration parameters. These include the *Header* panel where you can configure whether the group header is *Visible*, its *Label* the *Background* and *Text Color*. Click the minus in the header to minimize the group (and plus to expand a minimized group). The *Content* panel lets you configure whether the group appears as a *Panel* or *Cloud*, and its *Background* and *Stroke* colors. 
	Ungroup tool seperates all objects, lines, and labels and you can no longer move the objects in tandem.
	Clear tool empties the topology view.

Tool	Description
	Add tool open the Add a Graph Element window where you select the element type (Label, Cloud, or Linked View) and whether it is a static placement. Use the *Properties* panel to configure the font, background color, label contents, and so on, after you select the added element. **Note:** If you configure and save a Drill-in view with the design tools, then that view persists for all drill-ins from that device until you remove it an icon that appears between view Open and Save when it is enabled. Deleting such a drill-in view restores the default settings.  When you add these elements, you can elect to check *Static Placement* and they will not move with graphic elements when they are automatically re-arranged. You can, however, click and drag them.

Linked View

When you Add Element to a Linked View, the shortcut that appears onscreen provides a clickable link to the view you select when you add it.

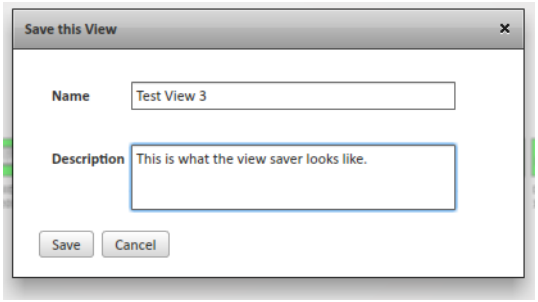


Use the *Properties* panel in the lower right corner of the screen to select the view, and configure the font on the link. The label is the linked view's title. You must create and save views before they are available to link.

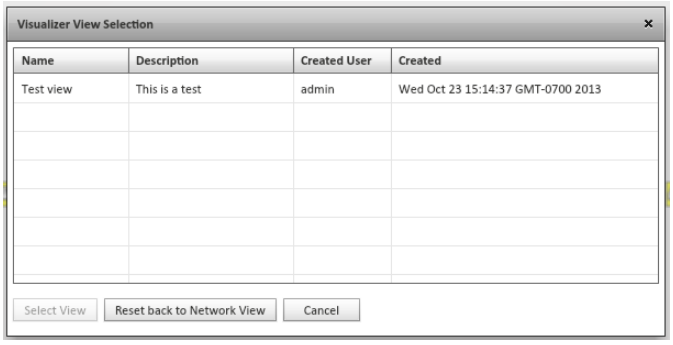
View

These icons let you save views you have configured, and has buttons to let you *Load a View*, *Save this view*, or activate *Edge Filtering* (links filtering).

Clicking *Save this view* displays a screen where you can *Name* and enter a *Description* for the view you are saving. Saving preserves node coordinates, background colors or graphics, and node sizes. The name of the current view appears on the right of the title bar for the Visualize My Network screen.



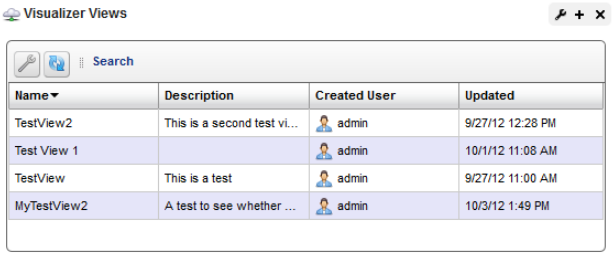
Clicking *Load a view* loads saved views selected from a screen. Users who do not own the retrieved view can save a copy.



You can also click *Select a View* to see the selected view, or *Reset back to Network View* to put the network view back to its default (all devices). You may have to refresh the page to see this button. *Cancel* dismisses this screen.

Visualizer Views

To see a catalog of available views, you can add this portlet to a page.



This lets you Edit the name and description of available views, and delete those you no longer need. You must open them in the Visualize My Network portlet.

Menu Options

Edit

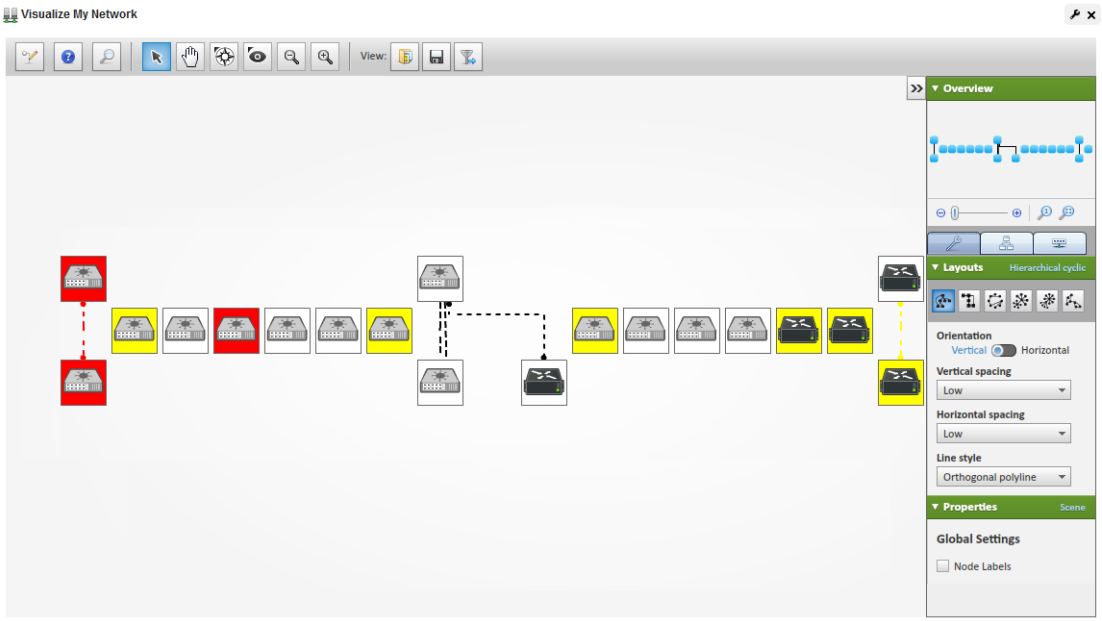
Add Resource Context

Export to Visio

Share with User

Configuring Views

Click and drag displayed portions of this screen to see other parts of the topology. To move the display more, click in the Overview Panel panel. You can also expand/collapse the panels on the left of the screen by clicking their title bars. (Figures below display them expanded.)



Nodes appear colored according to the alarm severity on the device, and white if no alarm exists for the device. Hover the cursor over an icon or link between icons to see a small screen describing its device (*Name*, *Type*, *IP address*), network status (*Responding/Not Responding*) and alarm severity. Click an icon to highlight it (or click its name in the Top-Level Nodes Tab tab list) and its connections to the network. See Alarms in Visualizations/Topologies on page 530 for more about the alarm severities indicated by icons in topology.

△ CAUTION:

If you installed a firewall on the application server, ports 80 and 8080 must both be open for topology to work.

NOTICE

If you have a Container View portlet on the same page as Visualize My Network, the selected container filters what appears in the view. Without containers, Visualize My Network configures what appears in other portlets on its page (for example Ports).

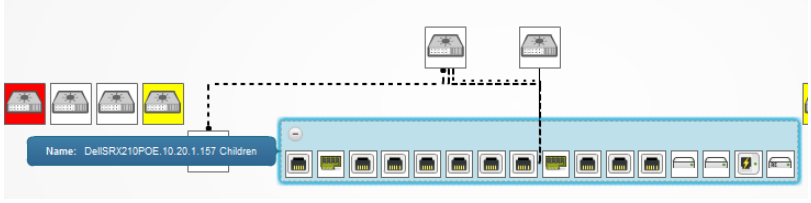
Click the Legend Tab to see the lines meaning, links, and alarm colors. Hover the cursor over a link to see its type described.

The screen to the right of the Visualize My Network screen displays the following panels:

- Overview Panel
- Layouts Panel
- Properties and Settings > Properties
- Legend Tab
- Top-Level Nodes Tab

Click the triangles to the left of these panels' labels to collapse or expand them.

In addition to the screen components immediately displayed, you can right-click an icon or component, and *Drill in* or *Expand* a device to see its subcomponents. If you expand, then its subcomponents appear with the rest of the topology. If you *Expand Grouped*, then the subcomponents appear in a minimize-able block (hover your cursor to see the block in color, and click the circled minus to minimize the group).



If you drill in, other components do not appear. In addition, you can select the Details menu option to open another browser window with the selected node's Details. The Event History menu item also opens a new browser window with the selected node's event history.

NOTICE

If you want to initiate Actions on a node or its components, do so by right-clicking the *Details* screen's Reference Tree.

The Layouts Panel selections determine the arrangement of such expansions or drill-ins.

When you drill in, the path back to the top level appears below the topology.

Click the level where you want to "drill out," or click *Home* to go to the top level.

If you right click the blank area of the screen, you can *Export* it as either a .png image or GML (graphic markup language), or print the displayed topology.

You can also right-click to *Remove Node* and delete a device from a view. You cannot add nodes to a view; you must add them when you create the view. You can visualize Managed Resource Groups, however, or simply Ctrl+click in the expanded Managed Resources portlet and right-click after your selection to Visualize the selected.

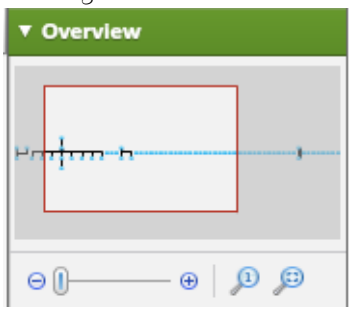
NOTE:

Because Topology uses Adobe Flash, menu items appear for that software when you right-click nodes. This includes *Settings, Global Settings* and *About Flash* menu items. The text below does not discuss these since they relate to Adobe products.

Overview Panel

The Overview panel displays a thumbnail of the entire topology view. Click on a location to center on it in the topology view.

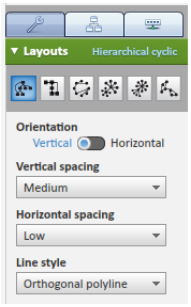
Use the slider at to change the magnification of your view. The icons to the right of the slider let you click them to fit visible icons vertically and both vertically and horizontally. You can also click and drag the cursor within this overview to change the magnification.



Layouts Panel

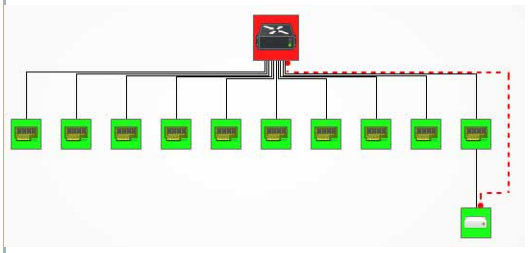
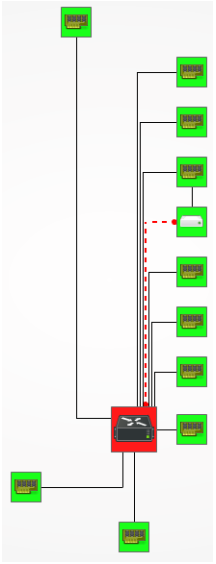
The Layouts panel lets you select and configure the automated node layout type that appears in the topology display.

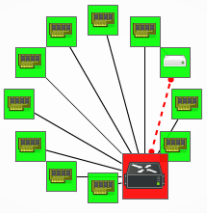
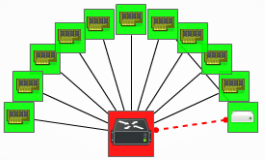
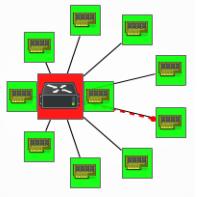
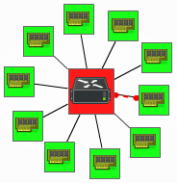
Access this panel by selecting the Properties and Settings > Layouts tab.



Use one of the following layout tools to specify a layout type and its settings. The fields and options available depend on the layout selected.

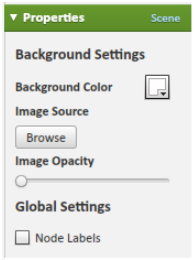
CAUTION:
Layout settings become fixed once you save a view. For example, when you save a view with a particular line style, that line style is not something you can alter later. Saved Views do not preserve links if they include non-grouped containers (single node representations).

Layout Tool	Description
	Hierarchical-Cyclic layouts arrange connections in a hierarchy.  Use the following settings to alter its appearance: • **Orientation** (Vertical or Horizontal) • **Vertical Spacing** (High, Medium, or Low) • **Horizontal Spacing** (High, Medium, or Low • **Line Style** (Orthogonal polyline, Straight, Straight polyline, Curved polyline, or Orthogonal curved)
	Orthogonal layout connections include right-angles.  Use the following settings to alter its appearance: • **Grid Spacing** (High, Medium, or Low) • **Use Diagonal Edges** enables edges that have non-right angles

Layout Tool	Description
	Circular layouts arrange all nodes in a circle.  Use the following settings to alter its appearance: • **Layout Angle** (360 or 180) • **Nodes spacing** (High, Medium, or Low)
	Balloon layouts display links between managed objects in a balloon tree structure. The root is typically whatever device you expanded or drilled into.  Use the following settings to alter its appearance: • **Root/Child wedge angle sector** uses radio buttons to determine the angle (360, 180). The root sector determines how much of an arc around that root the child nodes fill. The child sector determines the orientation around the child nodes. • **Root selection policy** specifies the item you want at the center of this view (Directed [a pop-up appears with the remaining selections], Most closed/ surrounded/weighted). • **Equal angle distribution** specifies whether to distribute nodes at equal angles.
	Radial layouts arrange nodes in concentric rings.  Use the following settings to alter its appearance: • **Layout angle** uses the radio buttons determine the angle (360, 180). • **Root selection policy** specifies the item you want at the center of this view (Directed [a pop-up appears with the remaining selections], Most closed / surrounded / weighted).
	Organic layout produces a static GEM layout, withou any parameters to tune. 

Properties and Settings > Properties

This panel configures the view properties in the Visualize My Network panel. This panel has the



following fields (you must click the *Design Mode* icon in the upper left corner to see all of them):

Background Settings

Background Color—Click the icon to see a color selector where you can select the background color for the Visualize My Network panel.

Image Source—Click the *Browse* icon to select a graphic for the background.

Image Opacity—Use the slider to set the background opacity.

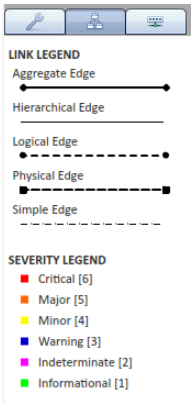
Global Settings

Node Labels—Check to label nodes in the Visualize My Network panel.



Legend Tab

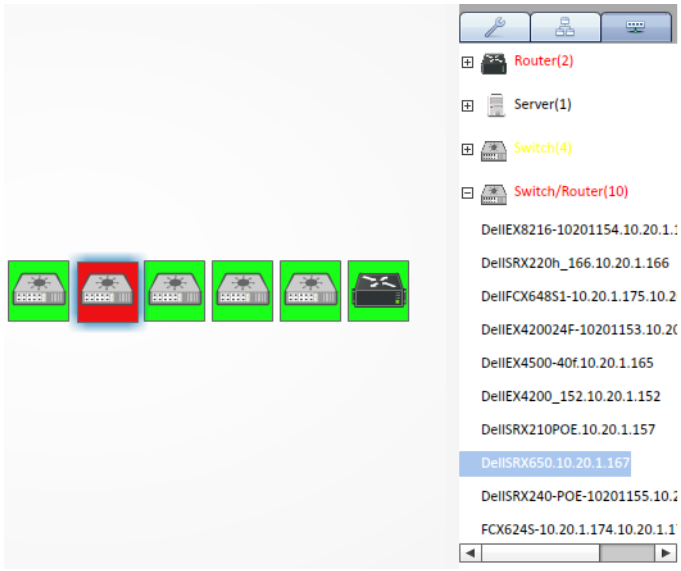
This displays the meaning of various link types and alarm severity colors in Visualize My Network



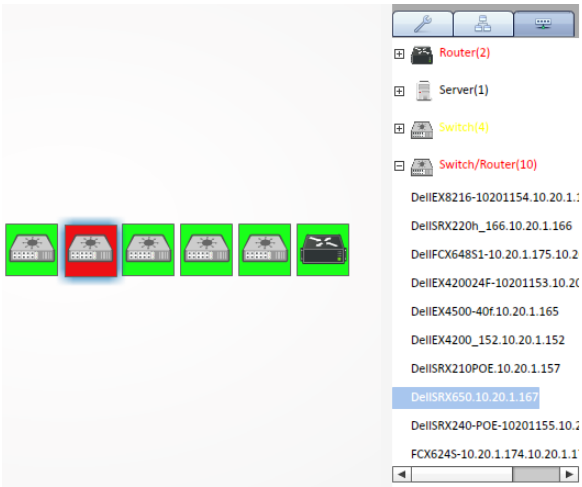
screens. It describes only the type of links that appear onscreen in the Visualizer.

Top-Level Nodes Tab

This displays a legend of icon types followed by a count (in parentheses) of how many of each appear in the topology. The switch at the bottom of this panel centers the display around the selected icon.



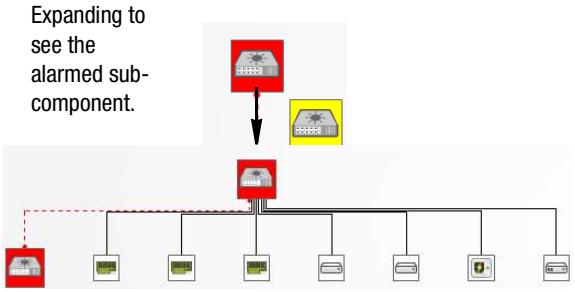
Click the plus (+) to the left of the inventory category icons to display a list of devices in that category in the topology. Click on a list item to highlight that device and its network connection in the topology view. A colored glow highlights it and its network connection(s). The listed inventory changes if you drill in.



The listed text appears in the alarm color of the device. See Alarms in Visualizations/Topologies on page 530.

Alarms in Visualizations/Topologies

Colored rectangles appear around topology nodes to indicate the highest alarm on them. Expand or



drill in to see alarms on the sub-components. For information about the alarm, hover your cursor over the device or subcomponent, and a tooltip appears describing the alarm's severity appears. The alarms indicated are like alarms described in the portlet Alarms Portlet on page 454.

By default, un-alarmed nodes appear clear / white. You can alter this so they appear green instead. To change this behavior, uncomment the `nodes.display.clear.severity.as.green=true` property in the `server-overrides.properties.sample` file in `\oware\synergy\conf`, and save the file as `serveroverrides.properties` in that directory.

Alarm Suppression in Topology Views

By adding icons to the devices in topologies, Visualize also displays the alarm suppression and maintenance status of devices in Visualizer views.



Here are the icons and their significance:

Icon	Device Status
	No icon—The device is unconstrained by the other Administrative States. Changing from Suspended to Normal stops alarm suppression. Standard access, and inclusion in right-to-manage count.
	Alarm Suppression active—Activated from the Managed Resources, Event Management pop-up menu option.
	Decommissioned — While this device is in inventory, it is not active. No device access allowed, no Monitor associations, no event processing, no Management Interfaces, no Authentication, no links, and no services are permitted.
	Down—The device is down.
	Maintenance — Neither alarms or polling apply to the device. Does allow resync and Adaptive CLI. Standard device visibility.
	Planned — Planned (future) device. No device access allowed, no monitor associations, and no event processing.
	Suspended — Suspends all device-related activities. No device access allowed, Monitoring Suspended, No event processing, Counts against right-to-manage.

You can set these alarm suppression and maintenance statuses in the right-click *Event Management* and *Maintenance* menus in the Managed Resources.

Links in Visualization

When you discover links between devices in your network (see Link Discovery on page 533), they show in the visualization view.

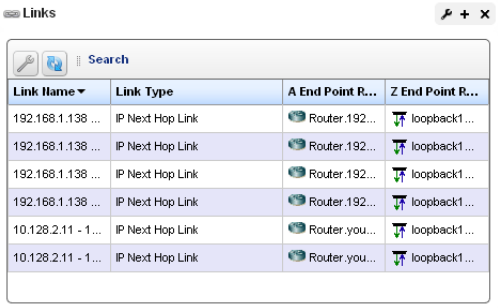


Hover the cursor over a link, and a panel the color of the link's alarm severity, appears with the link information (*Name*, *Type* (for example: Ethernet), *Severity*, and A / Z *Name*s for the endpoints).

OpenManage Network Manager currently does not support displaying one-ended links.

Links Portlet

The links portlet displays discovered or created links in your system. If information is truncated, hover the cursor over a column to see the contents of that column as a tooltip. The expanded portlet displays link connections in a Reference Tree snap panel, and includes columns for the interface and device for each end of the link.

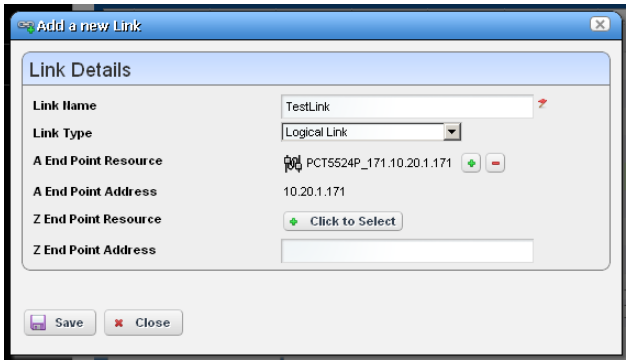


The expanded portlet displays link connections in a Reference Tree snap panel, and includes columns for the interface and device for each end of the link.

By right-clicking, you can create a *New* link, *Edit* an existing, selected one, or *Discover* links for specified devices. See New Link below, and *Link Discovery* on page 533 for more about creating, editing and discovering links.

New Link

When you create a new link or edit an existing one, the *Link Details* screen appears where you can configure the link.



This screen has the following fields:

Link Name—A text identifier for the link.

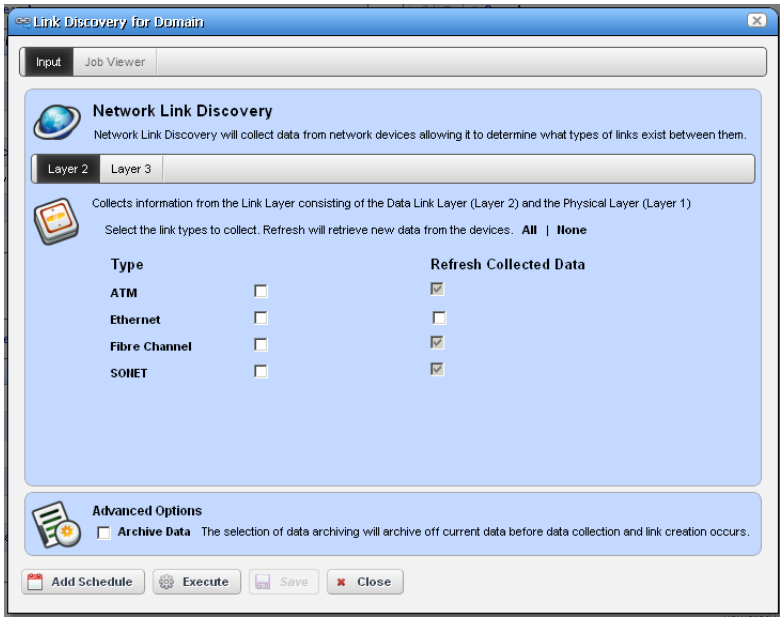
Link Type—Select the type of link from the pick list.

A End Point Resource / Address—Click the plus (+) to select a resource for one end of the link. When you right-click a selected resource, it automatically appears here. Click the minus (-) to remove it.

Z End Point Resource / Address—Click the plus (+) to select a resource for one end of the link. When you have selected two resources, they automatically appear as A and Z endpoints.

Link Discovery

This is an automated network link discovery feature that you can initiate from individual devices in the Managed Resources portlet, or with the *Link Discovery* button on the home screen. See Link Discovery Prerequisites on page 534 for a list of device features that provide link information. Links discovered can also appear in the screen described in Links in Visualization on page 531.



When you elect to discover links from a right-click menu, the *Network Link Discovery* screen appears. Check the type of links you want to discover or from which you want to refresh collected data. Other options available on this screen include the following:

Layer 2 / Layer 3 [checkboxes]—Select the layer for which you want to discover links. Depending on the layer selected, the available types appear as checkboxes below this tab selection.

NOTICE

Click *All / None* to select all or none of the displayed types for each layer. Remember, selecting more link types consumes more time and processing power.

Advanced Options

Archive Data—Checking this archives current data before collecting information about and discovering links.

NOTE:

Links with incomplete endpoint information are not discovered

Click *Add Schedule* to schedule link discovery, or *Execute* to run it now (and confirm you are willing to wait for results in a subsequent screen). The *Job Viewer* tab in the link discovery screen displays the message traffic between OpenManage Network Manager and the device(s). See Audit Trail Portlet on page 630 for more about Job Viewer screens.

Link Discovery Prerequisites

Although OpenManage Network Manager automates link discovery, you must enable the sources for link discovery information on the devices where you do such discovery.

Supported data sources used to derive links appear listed below.

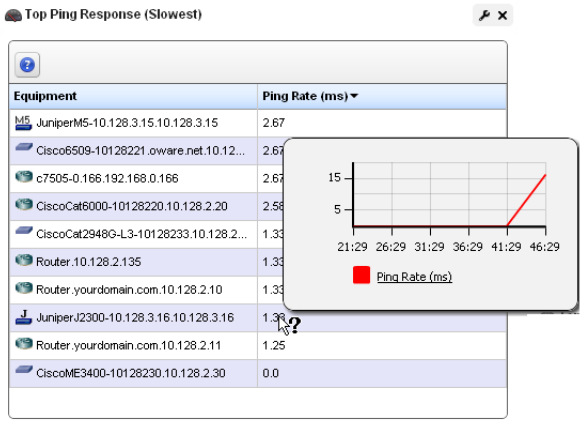
- IEEE Link Layer Discovery Protocol (LLDP) support
- Cisco Discovery Protocol (CDP) support

Performance Page

Use the Performance page to view the top asset portlets. The Performance > Monitors page displays Resource Monitors and Dashboard Views portlets.

Top *Asset* Portlets

The OpenManage Network Manager system uses seeded, default Active Performance Monitors (APM) to display performance data in several categories. The Top *Asset* portlets display device monitoring summary results. For example, the Top Ping Response (Slowest) portlet displays the devices that are the slowest to respond to a ping.



Devices listed are ranked by the monitored parameter. Hover over the Ping Rate column to view recent activity in a pop-up graph.

If you right-click a monitored item, you can select from menu items like those that appear in the portlet described in Managed Resources on page 454.

For some portlets (for example Top CPU/Disk/Memory Utilization, Top Interface Bandwidth/Errors), the right-click Performance menu items include Key Metrics. The menu can include *Performance*, which displays Dashboard Views related to the selected monitor.

For some packages, these can also include IP SLA statistics like the following: Top Bandwidth Received / Transmitted, Top CPU / Disk Utilization, Top Ingress / Egress Packet Loss, Top Jitter, and Top RT Delay. To see all available *Top* portlets, click *Add* > *Applications* and look below *Top N* on the subsequent panel.

Top RT Delay maps to the AvgRTDelay inventory metric. When no metric for Average RT Delay exists in the MIB, OpenManage Network Manager calculates it the average RT Delay using two MIB attributes: RTTSum (the total time taken for all round trips) and NumOfRTT (the number of round trips taken). The calculation of AvgRTT is the value of RTTSum divided by the value of NumOfRTT. OpenManage Network Manager maps this attribute to the AvgRTDelay inventory metric.

NOTICE

An alternative way to provide this kind of performance information is to use the Traffic Flow Analyzer. For systems generating large amounts of information that strain the limits of processing capacity, see Best Practices: Performance Tuning Traffic Flow Analysis on page 240 as a possible solution.

Calculations within Top N Portlets

The following Top N portlets are potentially available. Only those with monitored parameters display data. The data comes from monitor data using the monitor inventory mappings specified in each monitor.

The tooltip graph shows the values for the attribute over the last 30 minutes. The Errors and Discards attributes are counter values that show the change in value since the previous polling cycle. The other attributes are gauges which display a rate or percentage. The value displayed for each entry is the average over the last 30 minutes for the gauge attributes and the sum of values over the last 30 minutes for counter attributes.

These top asset portlets are available from the Performance page or can be added using the Add > Application menu option as needed.

The following portlets display data based on equipment targets:

Portlet	Description
Top CPU Utilization	Percentage of CPU used. Located on the Performance Summary page by default.
Top Disk Utilization	Disk use.
Top Memory Utilization	Memory use. Located on the Performance Summary page by default.
Top Ping Response (Slowest)	Lowest ping response. Located on the Performance Summary page by default.

The following portlets display data based on port or interface targets:

Portlet	Description
Top Interface Bandwidth	Most interface bandwidth use. Located on the Performance Summary page by default.
Top Interface Errors	Most interface errors. Located on the Performance Summary page by default.
Top Input Discards/Errors	Most input discards / errors. The tooltip/graph that appears when you hover your cursor over a row in these portlets shows the change in discards or errors, then the OMNM system adds changes to the base value and that sum appears within the table. Top Input Errors portlet is located on the Performance Summary page by default.
Top Output Discards/Errors	Largest number of output discards / errors. Top Output Errors portlet is located on the Performance Summary page by default.
Top Bandwidth Received/Transmitted	Displays percentage of bandwidth use received or transmitted.
Top Bandwidth Received (bps) / Transmitted (bps)	Displays bandwidth use in bytes per second. Located on the Performance Summary page by default.

The following portlets display data based on SLA or VRF targets:

Portlet	Description
Top Egress/Ingress Packet Loss	Most egress/ingress packets lost. Located on the Performance Summary page by default.
Top Jitter	Highest jitter rates
Top MOS	Highest MOS (a network performance measurement).
Top Packet Loss	Greatest packet loss. Located on the Performance Summary page by default.
Top RT Delay	Longest round trip (RT) ping delay

The following portlets are not monitor-based:

Portlet	Description
Top Problem Nodes	Devices with the highest alarm state
Top Configuration Backups	The most recent backups

Resource Monitors

Dashboard Views

Resources Page

The Resources page displays the following portlets by default:

- Managed Resources Portlet
- Connected Devices Portlet
- Search by IP or Mac Address
- Ports Portlet
- Interfaces Portlet
- Network Tools Portlet

Access the Resources page by clicking Resources from the navigation bar. The Resources menu provides access to the following sub-pages:

Sub-Page	Description
Discover	Displays the Discovery Profiles Portlet.
Actions	Displays the following: • Actions Portlet • Audit Trail Portlet

Managed Resources Portlet

(also located on the Home page)

Connected Devices Portlet

Connected Device(s) is an enhanced version of the Find Physical Connection for IP or MAC Address feature that was introduced in OpenManage Network Manager 6.1. As with the original Find Physical Connection for IP or MAC Address , SP1's Connected Device(s) can assist you in locating the port that a device you are searching for is physically connected to. Additionally, using Connected Device(s), you can determine everything that is connected to a specified managed device - whether those somethings are managed or unmanaged.

OpenManage Network Manager's Connected Device(s) feature works by utilizing LLDP, CDP, EDP, Bridging, and ARP data that is collected during Network Data Collection. At the very end of the Network Data Collection action, using that data, a list of connected devices is compiled and maintained for each device being managed by OpenManage Network Manager.

NOTE:

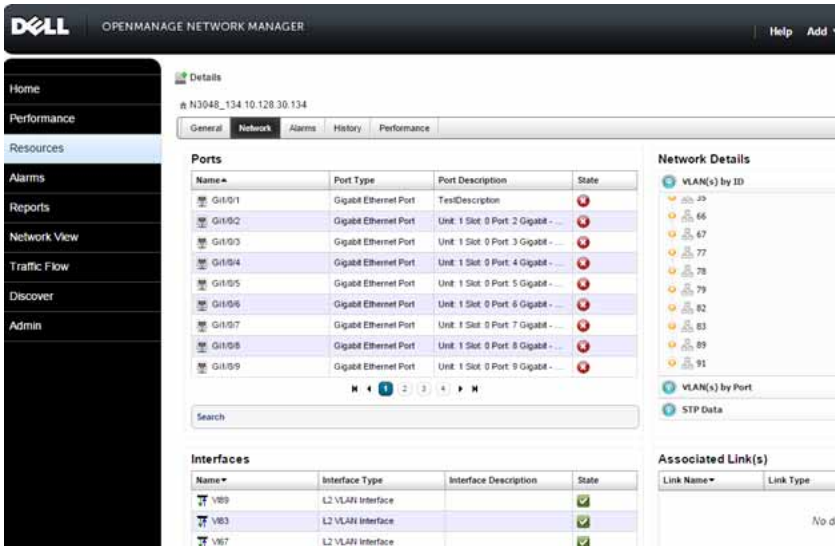
Connected Device(s) relies on Network Data Collection related data being up to date. It is automatically scheduled to be run daily, however - depending on your network situation - you may wish to schedule Network Data Collection to happen more frequently.

Additionally, when using Connected Device(s), if you have reason to believe that your Network Data Collection data may be out of date, it is suggested that you run Network Data Collection on any devices that you believe may have changed.

NOTE:

In order for the Connected Device(s) feature to have maximum success at finding devices that may be connected to your managed equipment, it is important to ensure that all devices in your network have all configuration necessary to enable the following applicable protocols/network technologies: LLDP, CDP, EDP, ARP, Bridging Tables. The necessary configuration varies from manufacturer to manufacturer, so please consult with the applicable guides for the devices you are working with.

Access this portlet from the Resources page or the selected connected device's Details portlet.



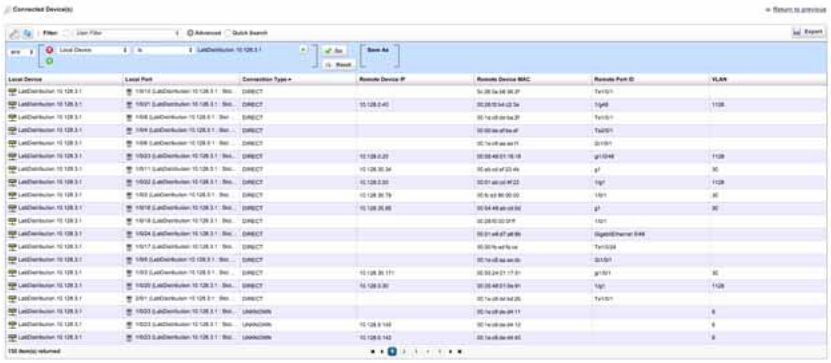
Searching and Filtering

Data displayed in the Connected Device(s) portlet can be searched and filtered on in two ways.

1 The Quick Search feature can be used from the minimized portlet view, and allows the user to search the Remote Device IP, Remote Device ID, Remote Port ID, and VLAN fields.



2 Advanced filtering can be done from the portlet's maximized view, and allows any field to be filtered on.



Fields

The following fields are available for Connected Devices:

- Local Device - The endpoint that is being managed by OpenManage Network Manager.
- Local Port - The port that the Local Device knows about the connected device through.
- Connection Type - This will either be DIRECT or UNKNOWN. If the type is DIRECT, the connection was discovered via LLDP, CDP, or EDP, and a direct connection is known to exist. In the case that the type is UNKNOWN, the connection was discovered via bridging data, and the connection may be either indirect, or direct.
- Remote Device IP - The IP Address of the device connected to Local Device.
- Remote Device ID - The Remote ID of the device connected to the Local Device. The value contained within this field can vary depending upon how LLDP, CDP, EDP, etc. is configured on the devices in your network (For example, it could be the MAC address of the remote chassis, or it could be a descriptive string).
- Remote Port ID - The Remote Port ID of the port that the remote device is connecting to the Local Device via.
- VLAN - The VLAN through which the Local Device knows about the Remote Device.

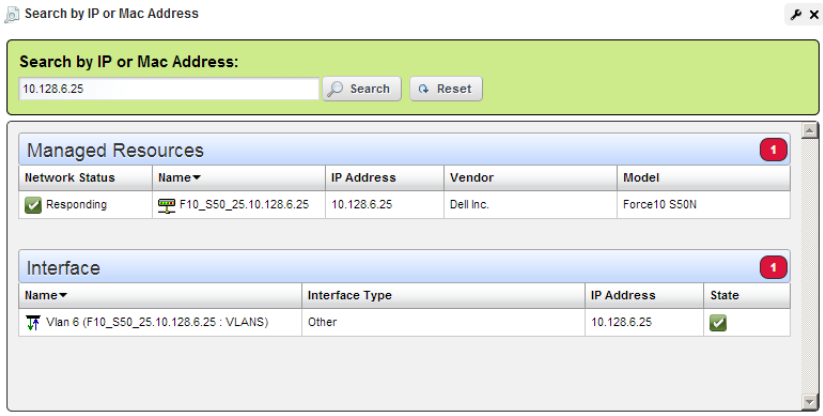
NOTE:

For a given connection, certain fields may or may not be populated, depending on which data (LLDP, CDP, EDP, Bridging, ARP) that connection was present in.

Search by IP or Mac Address

(also located on the Home page)

This portlet lets you find Managed Equipment, Ports and Interfaces for the IP or MAC address entered.



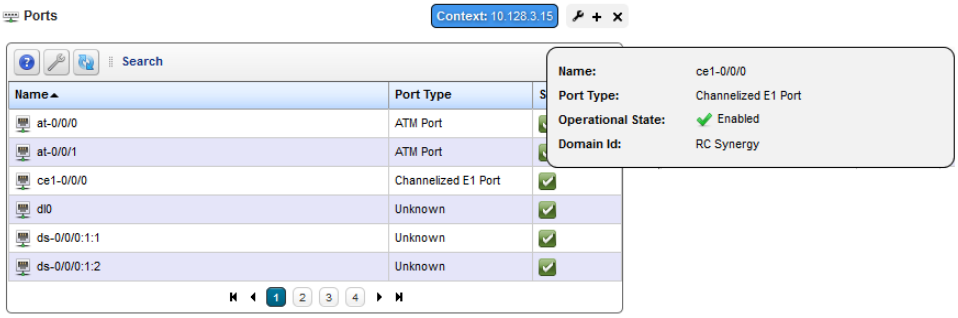
The same right-click menus as appear in Managed Resources, Ports Portlet or Interfaces Portlet appears in the search results. The display confines those results to what is found; if only ports satisfy the search criteria, then Managed Equipment and Interface do not appear. A count of found items appears in the upper right corner of each panel.

NOTE:

Search by IP or Mac Adress portlet supports search by description on both ports and interfaces

Ports Portlet

This summary portlet displays discovered device ports.



This displays a list of ports, with columns for *Port Icon*, *Equipment Name*, *Name*, *Type* and *Encapsulation*. Hover the cursor over the *State* column, and a popup appears to display the port's *Name*, *Type* and *Operational State* information. Right-clicking offers a subset of the actions listed in Managed Resources on page 454. You can also create links. See Links Portlet on page 531.

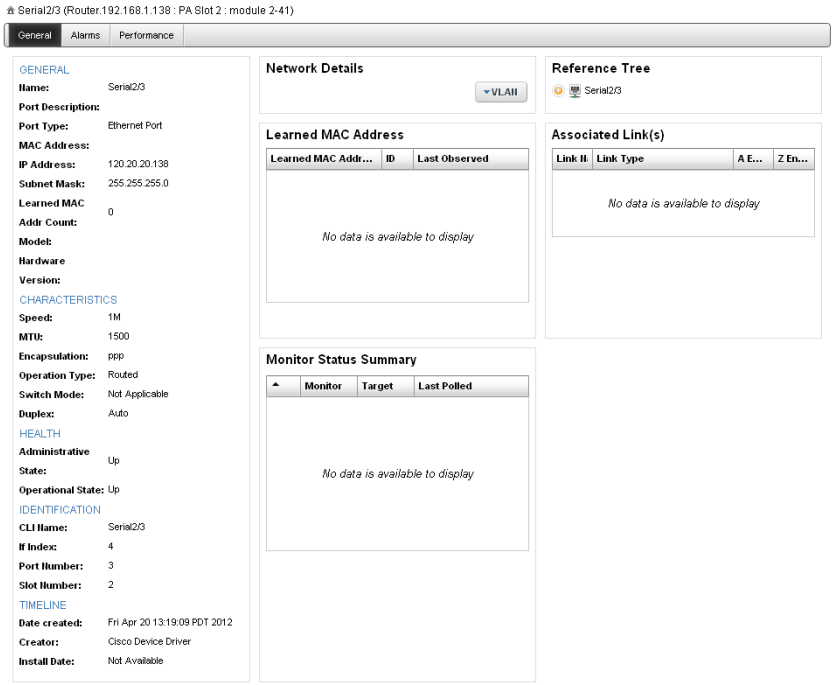
If the Ports summary portlet appears on the same page as the Managed Resources portlet, then a selection made in Managed Resources makes the Ports portlet display only ports for the selected resource. This "filter" through Managed Resources disables filters configured through the settings menu. See Understanding Containers on page 144 for more about this feature.

Port Details

This screen displays all the port's settings that have been retrieved, including a Reference Tree of logical interfaces below the port, a Learned MAC Address panel, Alarms related to the port, and other Detail.

NOTE:

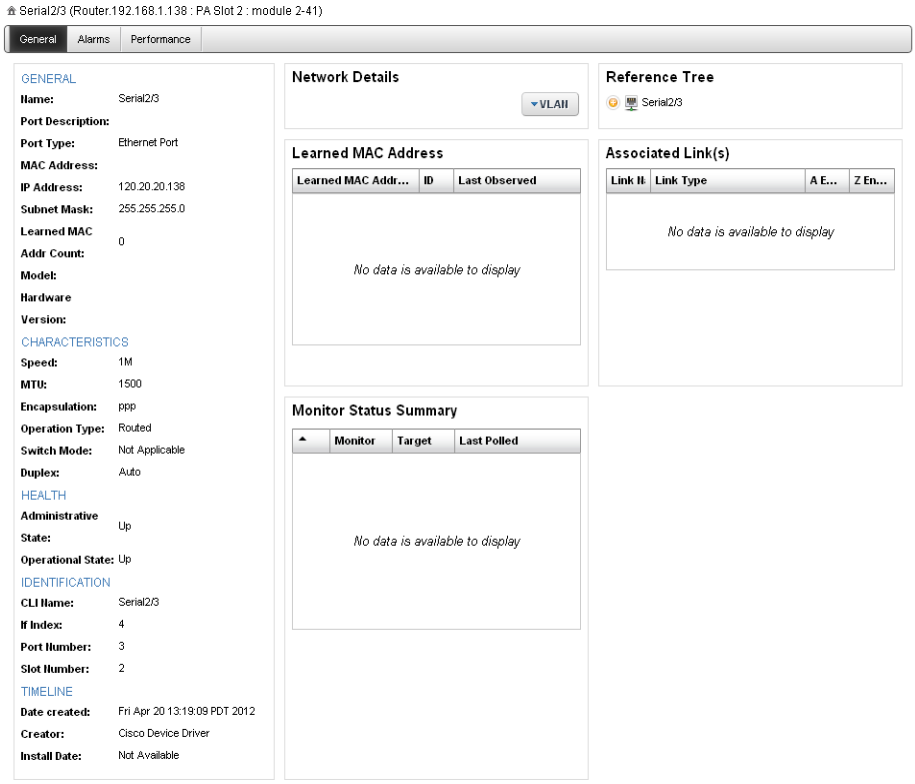
Switch Mode will only be populated for devices that support the Bridge-MIBs.The default value is unknown.



NOTE:

Switch Mode will only be populated for devices that support the Bridge-MIBs. The default value is

unknown.



This screen displays the following tabs, accessed by clicking their name in the top of the screen. Just above their names, a reminder appears of the name of the selected port.

General—In this tab, fields appear describing attributes for the selected port. For example *Date Created* (typically, this is the date discovered).

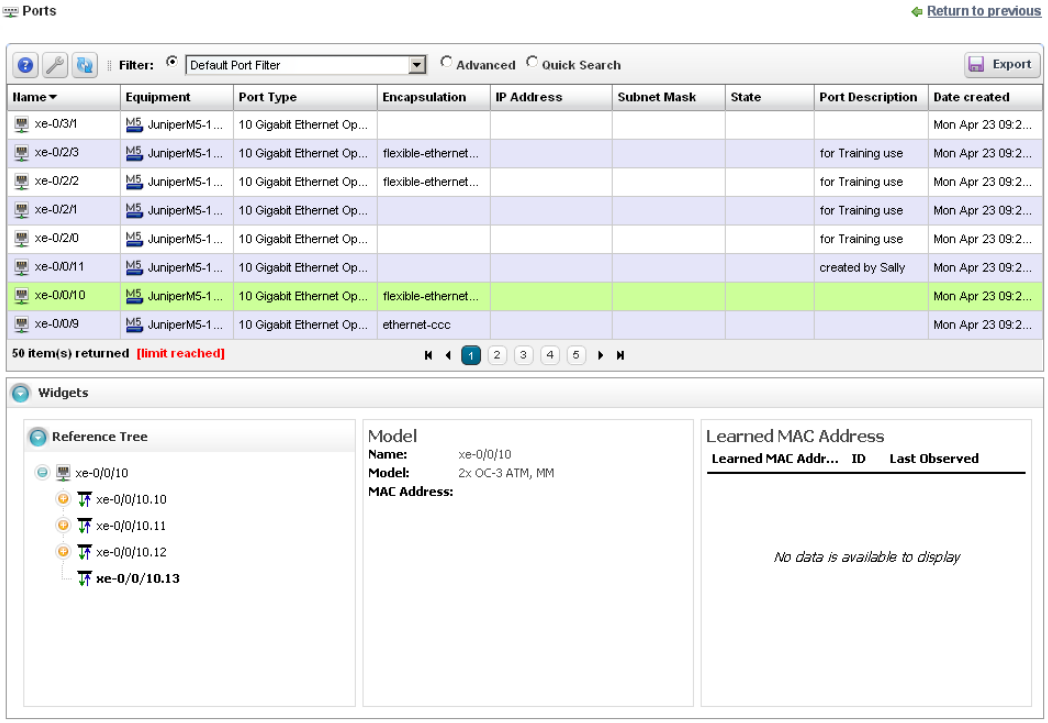
Alarms—This tab displays alarms and the Event History connected to the selected port. See Alarms Portlet on page 454 and Event History Portlet on page 482 for more about that information.

Performance—Displays monitor information, if available, related to the selected port.

See also Connected Devices Portlet on page 538 and Managed Resources Expanded on page 464 for an explanation of some of these fields.

Ports Expanded

Clicking the plus (+) in the upper right corner of the summary screen displays this expanded view of available ports.



The *Settings* button lets you configure columns that appear and their order. The available columns for this view include many related to the attributes that appear in Port Details on page 542, above. This screen also includes a *Reference Tree* displaying a tree of the selected port's relationship to logical interfaces and monitors.

This screen has columns similar to those described in Alarms Portlet on page 454. Configure these as visible or hidden by clicking *Settings*. The following are some additional columns available.

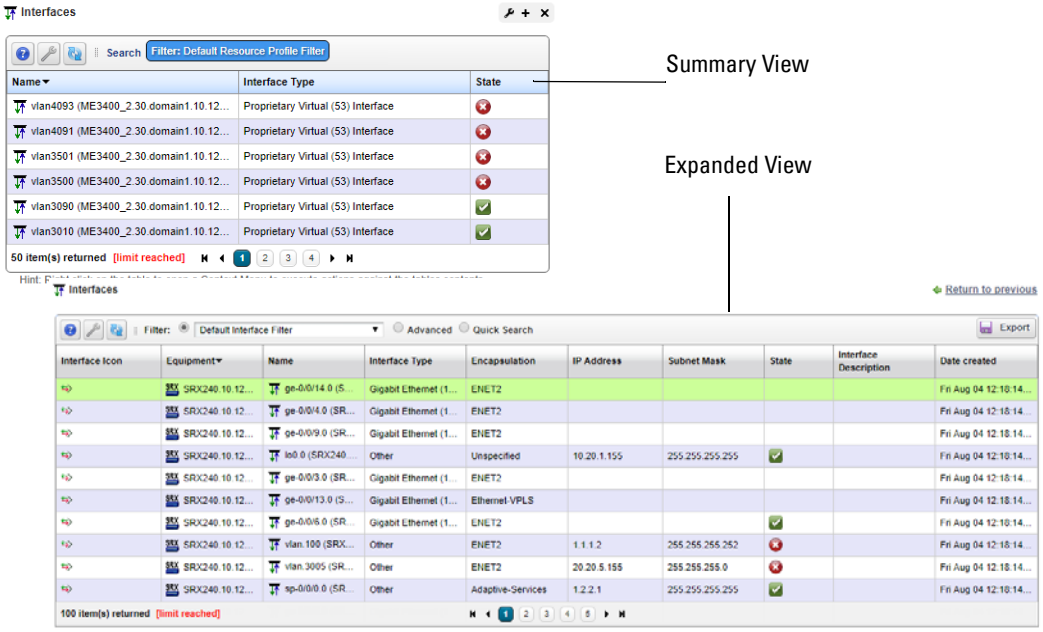
Interfaces Portlet

Interfaces

Use the Interfaces portlet to monitor and manage your discovered interface resources. This portlet, like the Ports Portlet portlet, displays subcomponents of discovered resources. However, unlike the Ports portlet it is not driven by a Managed Resources portlet selection on the same page where it appears. Also, unlike the Ports portlet, it does not display the Widgets panel in its expanded form, just more columns.

This portlet is intended for users who are interested in managing their discovered devices.

Access this portlet from the Resources page. This portlet has both a summary view and an expanded view. Each view could display different columns and could have the same pop-up menu options available.



Columns

Other than the general navigation and configuration options, the Interfaces portlets (summary and expanded views) include the following columns. The columns displayed by default are noted.

You can view the value for most of the hidden columns by clicking the Settings tool, selecting the columns tab, clicking Show for the appropriate column, and then applying the change.

Column	Description
Name	A interface identifier, such as the CLI Name. This field displays on the summary and expanded views by default.
Interface Type	The resource interface type, such as IP interface, Proprietary Virtual interface, Primary ISN interface, and so on. This field displays on the summary and expanded views by default.

Column	Description
State	An indicator that shows whether the operation state is functioning (checkmark) or not (X). This field displays on the summary and expanded views by default.
Interface Icon	The icon that represents this resource. This field displays on the expanded view by default.
Equipment	The name of the resource. This field displays on the expanded view by default.
Encapsulation	An identifier for the port. This field displays on the expanded view by default.
IP Address	The interface's **primary** address within the network. See Additional IP Addresses if you interface has more than one address. This field displays on the expanded view by default.
Subnet Mask	The network segment address to which an interface belongs. This field displays on the expanded view by default.
Interface Description	A detailed description for the interface. This field displays on the expanded view by default.
Date Created	The date this resource entered the database. This field displays on the expanded view by default.
Additional IP Addresses	Any additional IP addresses assigned to the interface, there than the primary IP address. For example, an interface might have an IPv4 address and a IPv6 address. If this is the case, the primary IP address appears in the IP Address column and the additional IP addresses appear in this column.
Administrative State	The interface's current administrative state, such as down, testing, unknown, or up.
Alarm Severity	The highest severity of any existing alarms against this resource.
Alarm Suppression Description	The description provided for an alarm suppression configuration.
Alarm Suppression Mode	A boolean setting (on/off). If Ad Hoc suppression is listed, the device does not receive alarms.
CLI Name	The command line resource name.
Container Index	The container index number.
Creator	The name of the person or process (such as a discovery rule) that created this interface.
Domain ID	The identifier for the interface domain.
Egress Bandwidth	The interface's outgoing bandwidth (bps).

Column	Description
Egress/Ingress Bandwidth Calculation	The type of calculation used to determine bandwidth: • CONFIGURED means that the OMNM system has a QoS policy configured against the interface. • TRUNK AGGREGATION means that the port is in trunking mode and calculates it bandwidth from its access ports. • INTERFACE AGGREGATION means that the total bandwidth of the parent is the sum of the bandwidth of it children if the interface has sub-interfaces. • ASSOCIATION means that the bandwidth is taken from the linked port if the port **is currently** UNCONFIGURED and has a physical and has a physical link to another port that **is not** UNCONFIGURED. • UNCONFIGURED means that the bandwidth is set to the port's IfSpeed. This is the default setting. See Bandwidth Calculation on page 216 for more details.
Foreign ID	An optional identifier for the customer's organization.
IfIndex	The SNMP interface index number used to identify a particular end point (port or interface).
Ingress Bandwidth	The interface's incoming bandwidth (bps).
Install Date	The time and date the interface was installed.
Interface Number	The number used to create a logical or virtual interface.
MTU	The maximum transmission unit (packet) size (256-9192).
Notes	A text field for information about the interface.
Port Number	A number assigned to user sessions and server applications in an IP network.
Rack Number	The number that identifies on which rack the component (card, port, or interface) is installed. This is useful when you have larger chassis that have internal racks.
RedCell.Config.Interface_VRFName	An identifier for the VRF.
Slot Number	An interface attribute set by the OMNM product.
Speed	The port/interface speed.
Subslot Number	The number that identifies which slot on the card that the service module is installed. Cards have the potential of supporting child modules, configurable service modules installed on the card.

Pop-Up Menu

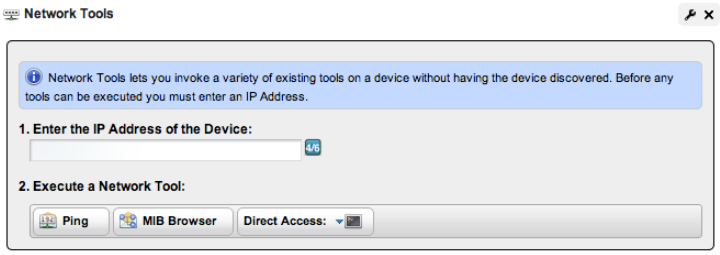
The Interfaces pop-up menu provides access to the following options. Right-click a row to access these options.

Menu Option	Description
Edit	Opens the Editing *interfaceName* window, where you view or modify the resources general details or interface properties.
Details (Click+Shift)	Displays the selected resource's general details and the alarms, event history, performance, and quality of service (QOS) details.
Visualize	Displays a topology map that includes the selected resources. See Using Visualization Tools on page 143 for more about these maps.
Domain Access Control	Opens the Domain Access Control window where you assign access rights to the domain.

Menu Option	Description
Actions	Executes any actions associated with the selected resource. An error is displayed if you do not have permission to execute actions or if there are no actions for the selected resource.
Event Management	Suppresses or updates alarms related to the selected resource. The following event management options available are: • **Start Alarm Suppression** starts alarm suppression after you enter a description and then click Start. A Success/Failure confirmation message is displayed. • **Stop All Alarm Suppression** discontinues all alarm suppression. A confirmation message is displayed. You can also stop alarm suppression using the View Active Suppressions option. • **Schedule Alarm Suppression** opens the New Schedule *suppressionAction* window, where you set the exception options and suppression targets parameters and then set the schedule options. • **View Active Suppressions** displays a list of active suppressions. A messages is displayed if there are no active suppressions. You can stop selected alarm suppressions from this list. • **View Event History** shows event history for the selected resource in the Event History portlet. • **Resync Alarms** refreshes the information displayed with the latest information in the database for the selected resource or all resources. Except for View Event History, perform these actions on one or more interfaces.
Links	Opens the Add a New Link window when you select New. Specify a link name, type, and A/Z end points resource/address. See Links Portlet on page 531 for more details about the link options available.
Show Performance	Shows performance data for the selected interfaces in the Performance Dashboard window. Click the edit tool to modify the dashboard view properties, entities, or attributes. See Dashboard Editor on page 227 for more about the editor and its options.
Traffic Flow Analyzer	Executes the following traffic flow analyzer actions on the selected resource: • Show Traffic • Create Configuration • Remove Configuration • Show Configuration See Traffic Flow Analyzer on page 239 for more details.
Edit Custom Attributes	Opens the Custom Attribute Editor where you define field characteristics, such as whether it is enabled, the label name, and the tooltip.
View as PDF	Creates an Acrobat PDF document containing this alarm's contents displayed in the summary portlet.
Share with User	Opens the Share with User window where you select the colleague you want to share this assets with and then type your message.

Network Tools

The Network Tools portlet lets you invoke a variety of existing functions on a device without having the device currently discovered. It typically appears listed as an available Application to install as a portlet.



Before you can use the tools, you must enter an IP address in the appropriate field. Once you have entered that address, you can use the following:

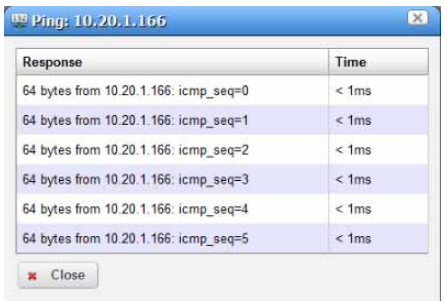
- Ping Tool
- MIB Browser Tool
- Direct Access Tool

NOTICE

If you want to restrict access for some users so they do not automatically log in with direct access, then remove direct access permissions for users, and use Network Tools for direct access.

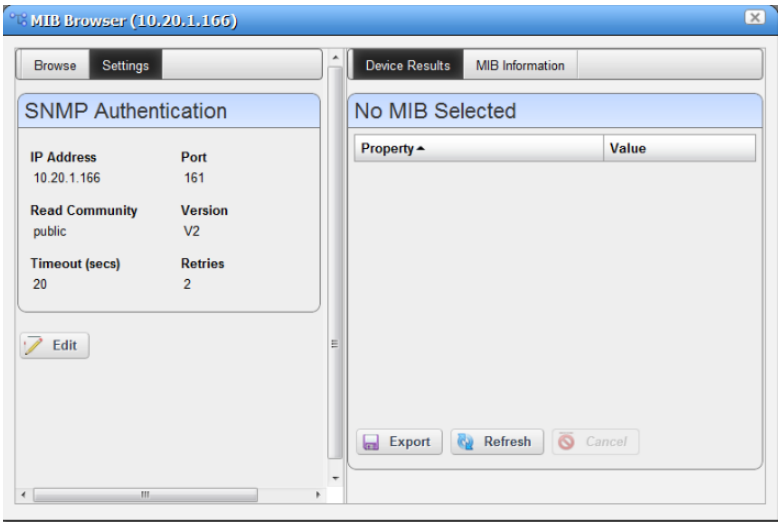
Ping Tool

The second button is the Ping tool, which pings the selected device, and lists the time for ping response.



MIB Browser Tool

The first button displays the MIB browser with default SNMP settings. You can *Edit* the settings to match the device's SNMP community settings and then save them. The next time Network Tools invokes the MIB browser, it defaults to your previous settings.



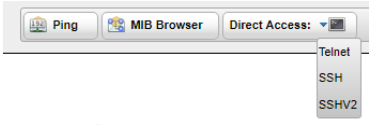
Once you are done editing the SNMP settings, click *Save*. Click the *Browse* tab to look through available MIBs as you would ordinarily do in MIB browser. See MIB Browser Tool on page 550 for more about using the MIB browser. You can also browse MIBs in the attribute selection panel for the SNMP monitor. See SNMP on page 212.

NOTE:

Locations for MIB file included with your package are subject to change without notice, but generally are under the owareapps/[application name]/mibs directory for different application modules. Refer to the *Installation Guide* for additional information.

Direct Access Tool

The third button on the Network Tools portlet toolbar opens the Direct Access tool. It provides a command line interface terminal for Telnet, SSH, and SSH V2 access to the device.



Click and select the type of direct access you want.

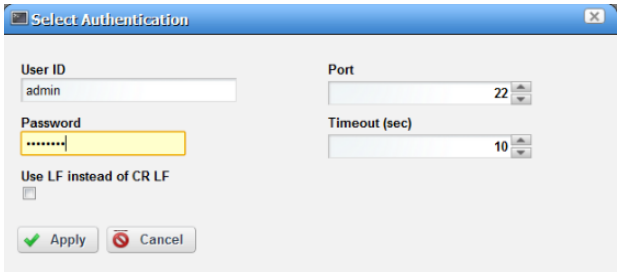
- Direct Access - Telnet
- Direct Access - SSH/SSH V2

Direct Access - Telnet

Telnet direct access connects to the device with telnet and displays the terminal session. You must login to the device manually, unlike the method described for discovered devices in Direct Access on page 467.

Direct Access - SSH/SSH V2

Direct Access for SSH or SSH V2 first prompts for a user name and password.



The *Use LF instead of CR LF* checkbox suppresses carriage returns when you click Enter key. This is necessary for some devices (for example: some Dell Power Connect devices).

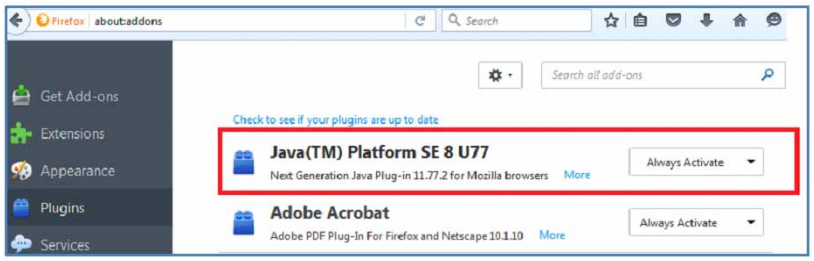
Once you log in, OpenManage Network Manager attempts to connect with SSH or SSH V2 using the user id and password provided. Some Dell Power Connect devices do not log when connected and prompt you to enter the user and password again.

Firefox Browser Configuration for Direct Access

To make Direct Access - Terminal tool for CLI cut-through to work on the Firefox browser; you must install or update the latest version of Java that is compatible with the browser from the following page.

https://www.java.com/en/download/manual.jsp

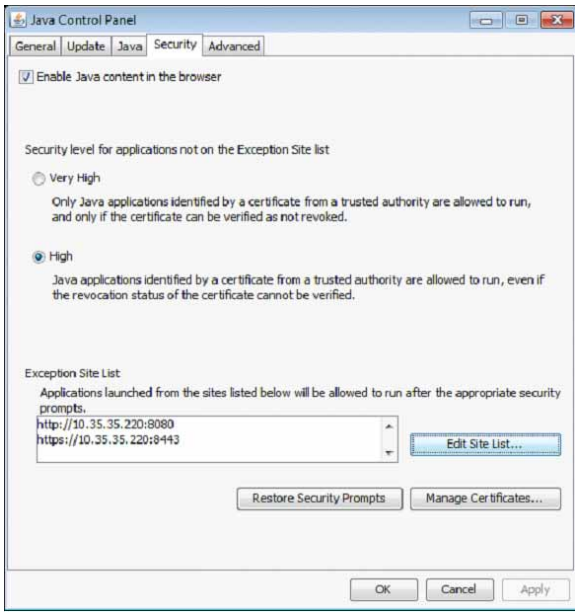
Once installed, go to Firefox plugins page (about:addons) and enable the Java plugin.



You must enable Java content in the browser from your Java Security configuration.

Control Panel > Java > Security tab > select "Enable Java content in the browser" option.

You might also have to add the OMNM server IPAddress to the Java Security Exception Site list.

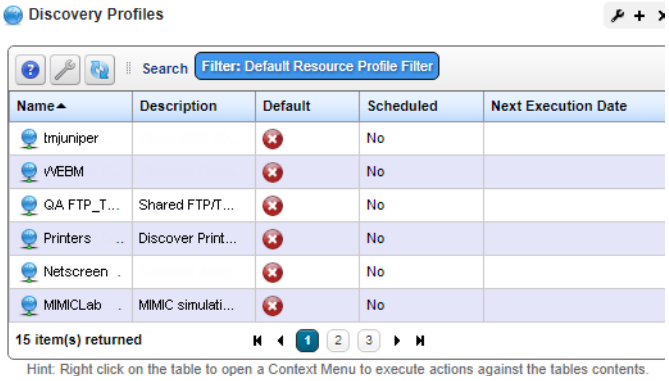


Discovery Profiles Portlet

select Resources > Discover

Discovery profiles configure equipment discovery for OpenManage Network Manager.

These profiles configure equipment discovery for OpenManage Network Manager.



The summary view displays the *Name*, *Description*, *Default* (the green check indicates the default profile), whether the profile is *Scheduled* and *Next Execution Date* for scheduled discovery.

The Expanded portlet adds a Reference Tree snap panel that displays a tree of associations between selected profiles and authentication and tasks that they execute. See Discovery Profiles Portlet on page 552 for more about this portlet.

You can import discovery profiles to target multitenant domains with a command line importer. The command is `importprofiles` and is in the `owareapps/redcell/bin directory.` This command takes the import file name an argument. The required domains should be available in the OpenManage Network Manager system before import occurs. Before importing discovery profiles to domains, any referenced authentications should be available in the domains or should be imported first by using the `importauths` command (the same way you would import discovery files). In other words, you should either manually create authentications for domains or import authentication files using importauths command before importing discovery files to those domains. Example XML files (with the `<customer>` tag for domains) are in `owareapps\redcell\db.`

NOTICE

The date format follows the operating system's conventions for the location and language selected. Restarting the system changes system menus to the new language. If you want to revert back to the original language in Linux, you may also need to update the cache file under `/var/cache/gdm.`

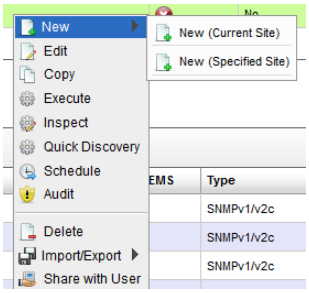
When OpenManage Network Manager discovers unknown devices, it examines the RFC1213 MIB for hints of the device's capabilities, determining if it looks similar to a layer 3 router or a layer 2 switch. Since some device can do both, OpenManage Network Manager classifies such ambiguous devices as routers. See Base Driver on page 66 for more about generic discovery capabilities.

Menu Options

When you right-click a profile, the following menu options appear:

New—Opens Discovery Profile Editor in new profile mode. (see General on page 555)

If you have the multitenancy option installed, you can limit a discovery profile to a tenant site or have it discover devices within the entire system. To create discovery profiles for a particular site, select the site with *New (Specified Site)* right-click menu item for the Discovery Profile portlet.



Edit—Opens Discovery Profile Editor.

Copy—Opens Discovery Profile Editor, and renames the selected profile as "CopyOf[Original Name]". Rename this copy appropriately before proceeding.

Execute—Executes a discovery profile. This also produces an audit trail (see Audit Trail/Jobs Status on page 689). A message appears indicating the success or failure of discovery execution.

Discovery execution continues in the background even when you close the audit trail / jobs screen, but the message indicating success / failure still appears when the discovery process is done.

Inspect—This validates that the device responds to ping, the profile's credentials, and that the device is licensed for discovery. See Inspection on page 559.

Quick Discovery—Opens discovery wizard displaying network and authentications, but without the Actions and Inspection panels. Not only does the Actions not appear, Quick Discovery does not execute any Actions. It is important to note that Quick Discovery settings, including Authentications and temporary device mappings, are not persisted. Device authentication mappings are only persisted in saved Discovery profiles. Click the Execute button once you open this screen to quickly discover equipment. See Network on page 556 for more about the screen this displays. Quick discovery is not available on tenant sites in a Multitenant system.

NOTE:

When using Quick Discovery, a "Quick Discovery" profile is created in Discovery Profiles. Quick discovery is intended to minimize user inputs by eliminating some data entry. For example, there is no description field and profile will have a blank description field. Users can edit the quick discovery profile and set a description, but the profile will be overwritten with the execution of the Quick Discovery process. It is important to note that Quick Discovery settings, including Authentications and temporary device mappings, are not persisted. Device authentication mappings are only persisted in saved Discovery profiles

Schedule—Opens schedule editor where you can create and/or modify the schedule for a discovery profile's execution.

Audit—Displays audit trails for the selected profile. See Audit Trail/Jobs Status on page 689.

Delete—Deletes a discovery profile. After confirming that is what you want to do, a notification message appears when deletion is completed on the application server.

Import/Export—Export the selected config file to disk, or import it from disk. You can also import/export a selected configuration file.

Provides the following actions when available for the selected image:

- Import retrieves a file containing XML compliance descriptions. Some imports can come from a URL.
- Export Selection exports the selected description to an XML file.
- Export All exports all descriptions to an XML file.

Click Download Export File to specify where to save the file.

The Import/Export option is useful as a backup or to share descriptors with other projects.

You must import data into the correct portlet. For example, you cannot import event data into the Actions portlet.

If one type of data depends on another, you must import the other data before importing the data that depends on it.

Share with User—Opens the Share with User window where you select the colleague you want to share this assets with and then type your message.

NOTE:

OpenManage Network Manager discovers Aruba Access points through the controllers to which they connect, discovery does not find stand-alone access points.

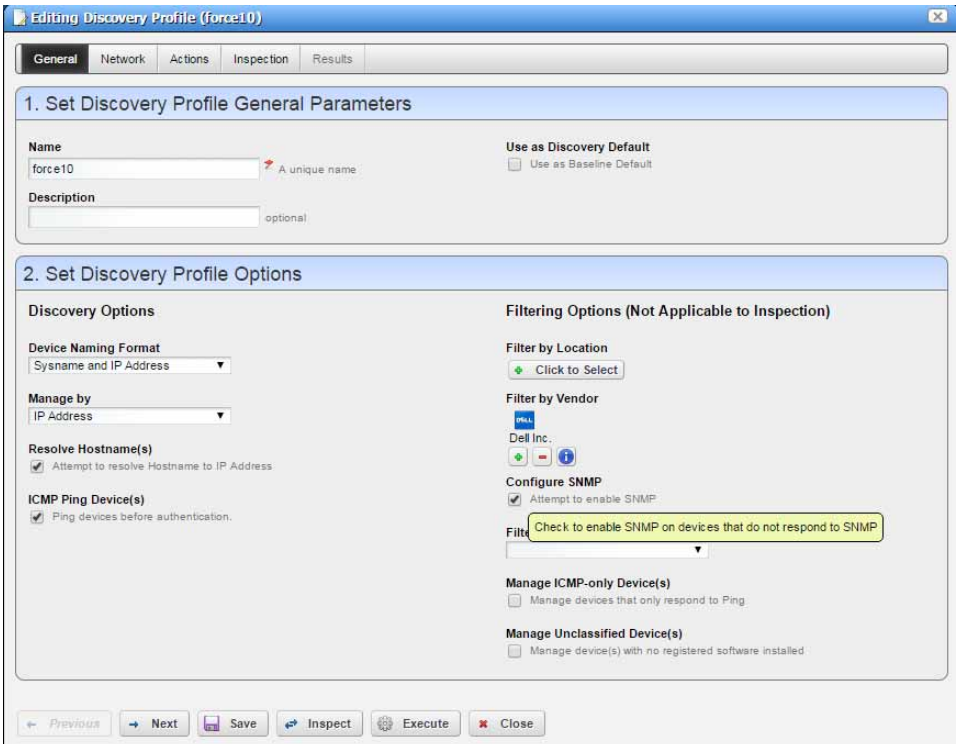
Discovery Profile Editor

This editor lets you create or modify profiles. It has the following sub-sections:

- General
- Network
- Actions
- Inspection
- Results

General

1 **General Parameters**—Set the *Name*, *Description* and a checkbox to indicate whether this profile is the discovery default.



1

2 **Profile Options**—Select the *Device Naming Format* (how the device appears in lists, once discovered), whether to *Manage by IP* address or hostname, and check whether to *Resolve Hostname(s)*, *ICMP Ping Device(s)*, *Manage ICMP-only Device(s)*, or *Manage Unclassified Device(s)*. This last checkbox determines whether OpenManage Network Manager attempts to manage devices that have no OpenManage Network Manager device driver installed. If your system's license permits it, such management may be possible, but more limited than for devices with drivers installed.

If your license limits the number of devices you manage, discovering such "generic" devices may count against that limit. See Base Driver on page 66 for more.

The Filters (by *Location*, *Vendor*, or *Device Type*) let you narrow the list of devices discovered by the selected item(s). As the screen says, this filtering will not have any impact on the processing that occurs during the Inspection step.

The checkbox labeled "Attempt to enable SNMP" is visible if a vendor has been selected. If this checkbox is selected, if a device is not reached during the SNMP discovery process, the discovery engine will attempt to enable SNMP on the device using the SNMP credentials

provided in the authentication section of the discovery profile. In order to enable SNMP on the device the device must be reachable via CLI with the CLI credentials provided. If the device is successfully enabled for SNMP the SNMP discovery process will be reattempted.

NOTE:

Fields like *Location* query the database for current information, so even though its field may appear empty, Locations may exist. Click the Search button to the right of this field to populate it. Keeping such fields empty until you use them enhances performance.

The buttons at the bottom of the Profile Editor let you navigate through this series of panels. *Previous* / *Next* move back and forth between screens, *Save* lets you preserve whatever stage you have configured, and close the editor, *Inspect* moves directly to the Inspection screen (described below), and *Execute* triggers the discovery profile and opens the Results panel, displaying message traffic between OpenManage Network Manager and the device(s). Click the "X" in the top right corner of these screens to close them without saving.

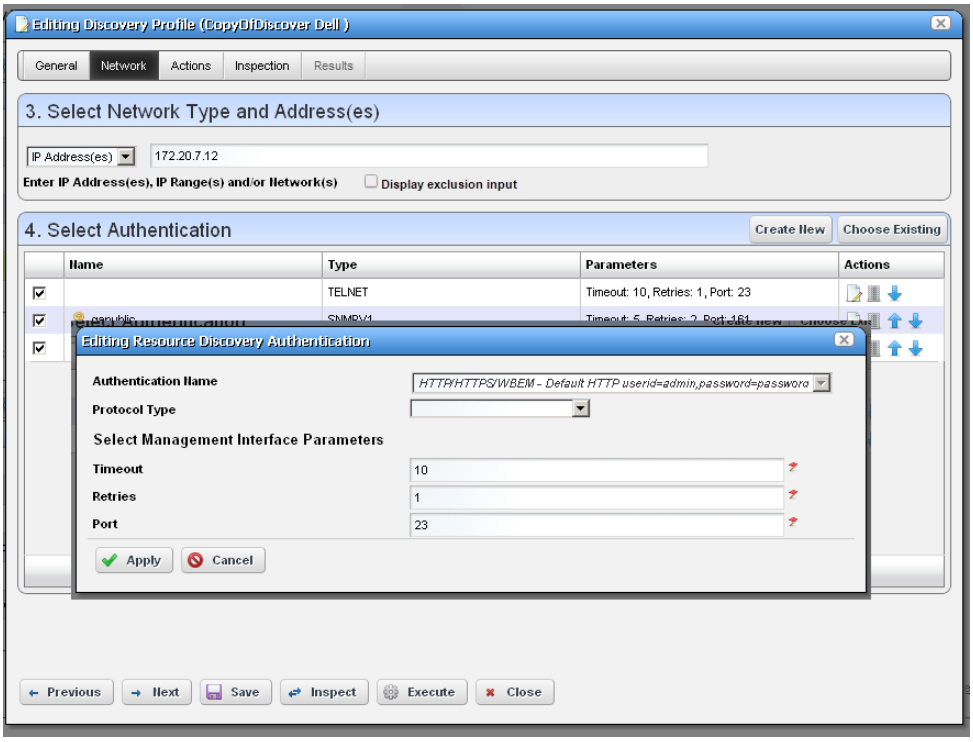
If you discover devices without retrieving their hostnames, and need that hostname later, you can re-run discovery after checking *Resolve DNS Hostnames*. This fetches the DNS hostname and resyncs the device.

Network

The Network Panel collects the network (IP range, hosts, and so on) and the authentication information for the discovery profile.

3 After you click *Next*, the *Network* panel appears.

Network Type and Addresses—Select the type of entry in the pick list *(IP Address(es)*, *CIDR Address*, *Hostname*, *SNMP Broadcast*, *Subnet)*.



The tooltips tell what valid entries look like.

NOTE:

OpenManage Network Manager now discovers all IP addresses in a specified range, regardless of the specified base IP address is (middle, starting IP, or last in the range). IP addresses outside of range will not be discovered. You can use the CIDR specification of the network to discover rather that the subnet ID.

You can exclude IP addresses, or ranges of IP addresses if you check the *Display exclusion input* checkbox and input the addresses you want excluded as you did for those you entered in the *Address(es) for Discovery* field. Such exclusions only apply to the profile where you enter them. To exclude an address or range, use the `com.dorado.redcell.discovery.exclude` property. Examples of how to enter such exclusions appear in the `redcell.properties` file under `owareapps\redcell\lib`. As always, best practice, if you want such properties to persist is to put the property in `owareapps\installprops\lib\installed.properties`.

4 **Authentication**—You can create new, or add existing authentications. See Authentications Portlet on page 628 for the way to create such authentications outside the discovery process.

CAUTION:

If a device or its driver requires two authentications and you only enter one, it may not appear in inventory after discovery. To correct this, enter both authentications in the Discovery Profile or in Quick Discovery. If you discover a device partially with only one authentication—typically the SNMP community—you can re-discover with the correct authentications later, or *Edit* the resource to add that correct authentication *and* the management interface for it.

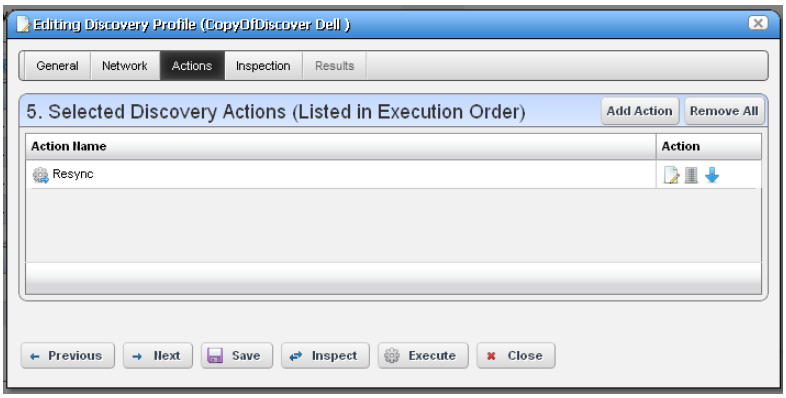
Notice that authentications appear with *Edit* / *Delete* icons and *Up* / *Down* arrows on their right. The *Edit* icon opens the authentication editor. Click the arrows to arrange the order in which the application tries credentials (top first). Ordering only applies when two credentials are of the same type.

If you have imported a discovery profile without importing or creating the authentications it uses, editing its authentications is not possible. If you cannot import authentications, or have not created them when you do attempt to edit them, the easiest solution is to delete the un-imported un-created authentication the profile refers to and create a new one.

If two similar authentications include one with a “deeper,” enable login, and a “shallower” one without that additional login, arrange to try the deeper login first. If the device rejects it, discovery still tries the shallower one later.

Actions

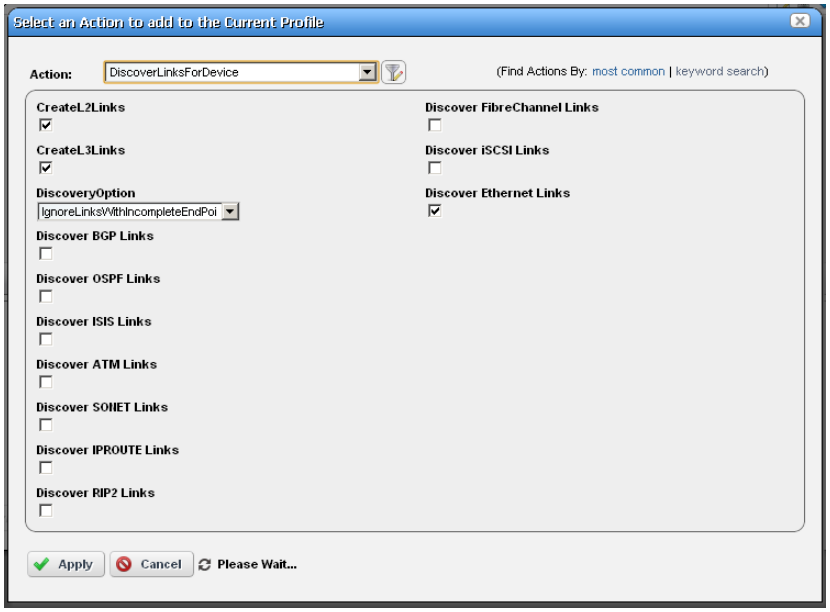
5 When you click *Next*, the *Actions* panel appears.



You can simply accept the default actions that appear here (like *Resync*, adding the device to a global *Scheduled Resync*, link discovery, and so on) by clicking *Next* to the Inspection portion of discovery. (See also Configuring Resync on page 62)

Alternatively, you can do the following:

Add Action—This opens a screen with a selection list of available actions. Click *Apply* to select an action to add to the list for this profile.



Notice the default for this screen displays the *most common* actions, but you can also click *keyword search* in the top right corner to display a search field instead of a pick list with the most common actions. The search results appear in the pick list. When you select an item, if it has parameters, they appear listed below that item. Use the check-box(es) or pick list to configure these parameters, then click *Apply* to select this action as part of the profile. See for more about these.

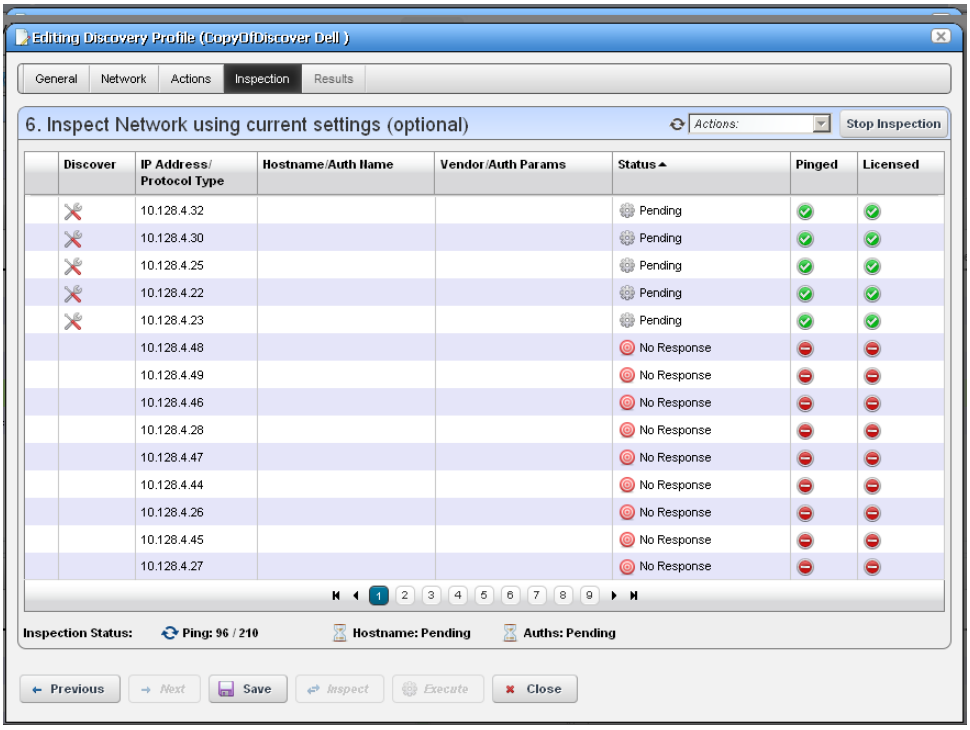
The screen appearance changes depending on the selected action.

Edit, Delete, Move—These icons appear to the right of each action. If you *Edit* a profile with parameters, you can change them. The screen looks like the one that appears when you *Add* actions. Deleting actions removes them from the list, and the *Move* arrows help arrange the order in which actions appear listed, and are executed. The list of actions the profile executes goes from top-to-bottom.

Inspection

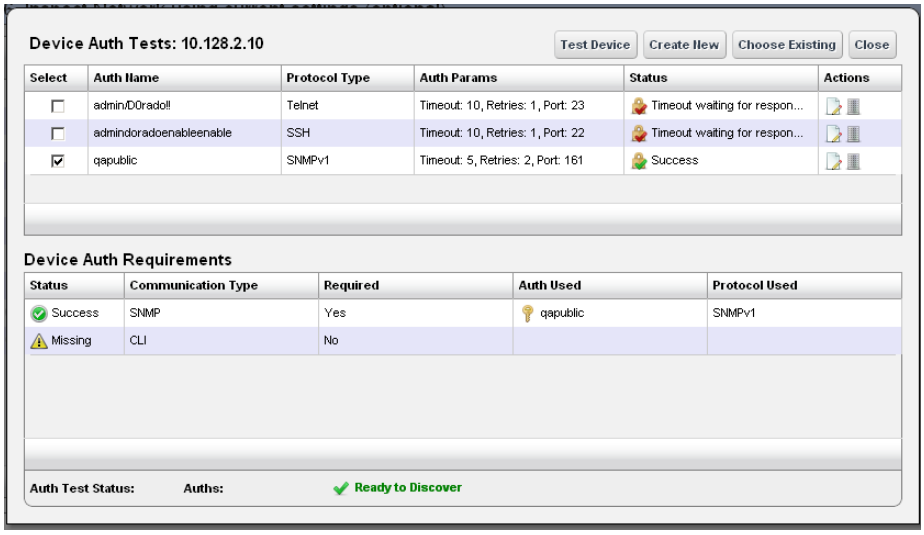
Using the Inspection Panel is an optional step. If you want to execute the profile after entering the required information on the General and Network panels, you can skip this step, and just click *Execute* at the bottom of the panel.

6 **Inspection**—This screen lets you preview the discovery profile's actions and access to devices. If you clicked *Next* rather than *Inspect* at the bottom of the previous screen, click *Start Inspection* in the top right corner of this screen to begin the inspection process that validates the device's credentials.



Notice that the *Inspection Status* fields at the bottom of the screen indicate the success or failure of Ping, Hostname resolution, and Authentications, and the *Status* column displays whether a valid authentication exists, whether it has been tested, and whether the test is successful.

When authentications are unsuccessful, click the icons to their right to remove or edit them. You can also click the wrench / screwdriver "fix it" icon in the *Discover* column to open an editor where you can revise the authentications for that device.



Clicking *Create New* lets you create new authentications, *Choose Existing* lets you select from existing authentications, *Test Device* lets you try out the authentications you have selected, and *Close* closes this screen. Notice that you can configure new or existing authentications' port, retry and timeout settings before you click *Apply* (or *Cancel*) in the authentication editor that appears after clicking the "Fix it" button.

7 **Save—**Click *Save* to preserve the profile. You can then right-click it to select *Execute*. If you select *Execute* from the profile editor, OpenManage Network Manager does not save the profile to execute later.

Results

8 **Execute**—Clicking *Execute* begins discovery, and the message traffic between OpenManage Network Manager and the device appears on the *Results* screen.

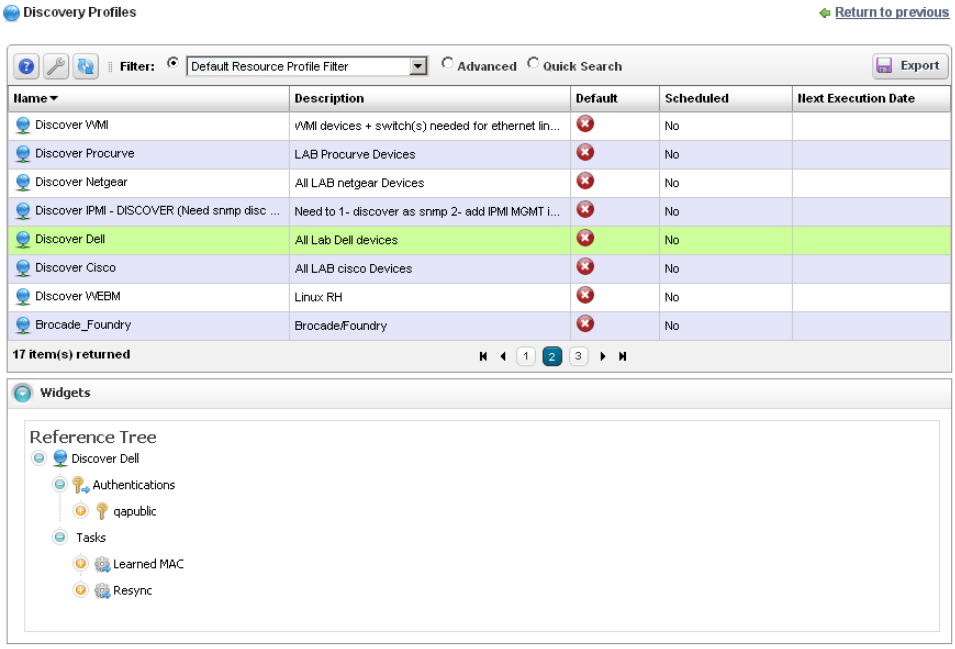
This opens a standard Audit Trail/Jobs Status window displaying the message traffic. See also Audit Trail/Jobs Status on page 689 for more about retrieving audit trail archives.

9 A message (*Discovery Profile Execute is complete*) appears in the *Messages* at the bottom left of the status bar.

10 Click the X in the top right corner of the discovery profile editor to close it.

Discovery Profiles Expanded

This larger view offers a *Reference Tree* snap panel where you can see the connection between a selected profile and the authentications and discovery tasks it includes.



Actions Portlet

Resources > Actions

Action Groups Portlet

Resources > Actions

Configuration Management Page

The Configuration Management page displays the following portlets by default:

- Managed Resources
- Configuration Alarms
- Configuration Management Schedule
- Configuration Files Portlet
- Image Repository Portlet
- File Servers Portlet

Access the Configuration Management page by clicking Configuration Management from the navigation bar. The Configuration Management menu provides access to the following sub-pages:

Sub-Page	Description
Compliance	Displays the following portlets: • Compliance Policy Groups • Compliance Policies/Proscan • Compliance Schedules • Compliance Alarms

The OpenManage Network Manager ProScan change management utility lets you scan stored configurations or Adaptive CLI show command output to verify that managed devices comply with company, department, or industry standards. The ProScan utility also automatically tracks all changes to managed devices. You can report on user-specified values found in persisted backup configuration files for a group of devices. This lets network managers, security officers, and external auditors to generate detailed audit trail documents to validate compliance with both internal standards (ISO 17799, NSA Guidelines) and industry regulations (Sarbanes-Oxley, GLBA, HIPAA).

Compliance reporting lets you specify a text string, regular expression, or optionally the generated configlet from File Management (NetConfig) for matching. Group results must be separated by device like Adaptive CLI Manager. When ProScan policies run, the application emits notifications whose contents depend on whether compliance was or was not maintained.

NOTICE

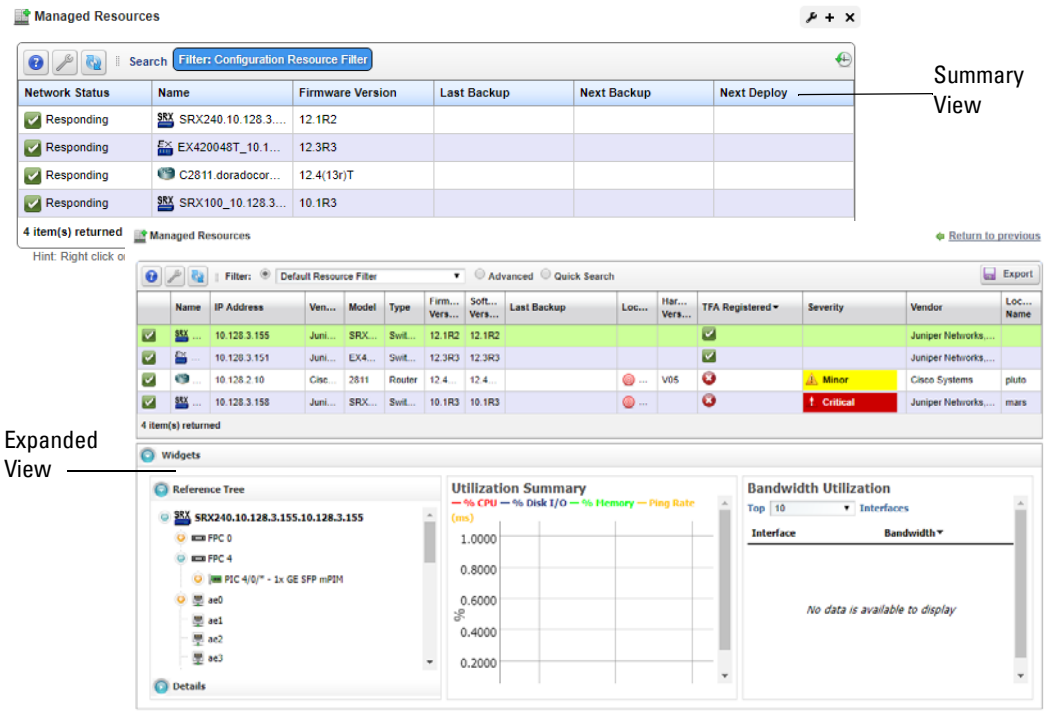
Your system may have several ProScan examples. You can use the examples as is, or copy and alter them to suit your network.

Managed Resources

Use this Resource Management portlet instance to manage the configuration of devices urations that you discovered or created on your network. Resource Management portlets show device-specific information, both general (name, type, location, contact) and technical (vendor, subcomponents, and so on). The default layouts in the summary and expanded views are geared towards device configuration management.

This portlet is intended for anyone that wants to manage their network device's configuration.

Access this portlet by selecting the Configuration Management page. This portlet has both a summary view and an expanded view. Each view displays different columns and have the same pop-up menu options available.



Columns

Other than the general navigation and configuration options, this instance of the Managed Resources portlets (summary and expanded views) include the following columns. The columns displayed by default are noted.

You can view the value for most of the hidden columns by clicking the Settings tool, selecting the columns tab, clicking Show for the appropriate column, and then applying the change.

Column	Description
Network Status	The resource's status in the network, such as: • **Responding** means that this application gets a response from the device through a network protocol. • **Not Responding** means that the device does not respond to the protocol. • **Indeterminate** means that the monitoring software has not tried to reach the device or there was some other error that prevented us from determining one of the other two statuses. The Network Status option availability depends on its response to the ICMP monitor. If you disable the monitor (for example, for performance reasons), a status may appear, but it is not meaningful. This field displays on the summary view by default.
Name	The device name. This field displays on the summary and expanded views by default.

Column	Description
Firmware Version	The version for the device's firmware. This field displays on the summary and expanded views by default.
Last Backup	The date and time that the device was last backed up. You can sort on this column. This field displays on the summary and expanded views by default.
Next Backup	The next date and time that the device is scheduled to back up. This field displays on the expanded view by default.
Next Deploy	The next date and time that the device is scheduled to deploy. This field displays on the expanded view by default.
IP Address	The device's IP address. This field displays on the expanded view by default.
Vendor	The vendor for this device. This field displays on the expanded view by default.
Model	The device model. This field displays on the expanded view by default.
Type	The device type, such as switch, router, and so on. This field displays on the expanded view by default.
Software Version	The version for the device's software. This field displays on the expanded view by default.
Location	The device's location shown with text and an icon. expanded view
Hardware Version	The device's version. This field displays on the expanded view by default.
TFA Registered	An indicator that the TFA is registered (checkmark) or not (). This field displays on the expanded view by default.
Alarm Severity	The highest alarm severity opened for a device. This field displays on the expanded view by default.
Vendor Name	The resource's vendor name. This field displays on the expanded view by default.
Location Name	The location where the resource resides. Shows both text and icon. This field displays on the expanded view by default.
Widgets	Additional information about the selected rule, such as: • Reference Tree • Details • Utilization Summary • Bandwidth Utilization The Widgets field is available only from the expanded view.
Additional IP Addresses	Any additional IP addresses assigned to the resource, other than the primary IP address. For example, a resource might have an IPv4 address and a IPv6 address. If this is the case, the primary IP address appears in the IP Address column and the additional IP addresses appear in this column.
Alarm Suppression Description	The description provided for an alarm suppression configuration.
Alarm Suppression Mode	A boolean setting (on/off). If Ad Hoc suppression is listed, the device does not receive alarms.

Column	Description
Asset Tag	Any asset tag identifier for the device.
Contact	Any contact associated with the resource.
Creator	The user or process (such as, a discovery rule or device driver) that created this resource.
DNS Hostname	The resource's host name.
Description	A text field for a description of the resource.
Discovery Date	The date and time the resource was discovered.
Domain ID	The identifier for the device's domain. This is populated in a multitenant environment.
Equipment Icon	An icon that represents the resource. You can edit to change this icon. Discovery assigns standard icons.
Foreign ID	An optional identifier for the customer's organization.
Install Date	The date and time that the resource was installed.
Last Configuration Change	The time and date for the last configuration change detected.
Last Modified	The date and time that the last modification occurred.
Last Status Change	
MAC Address	The resource's Machine Address Code.
Manage By Hostname	An indicator that shows whether the device is managed by host name rather than IP address.
Management State	The management state of the resource.
Mediation Server 2 IP Address	The resource's secondary mediation server IP address (applies in a high availability system with two mediation servers).
Mediation Server IP Address	The resource's mediation server IP address.
Next Restore	The next date and time to restore a resource.
Notes	A text field for information about the resource.
Operational State	The resource's state independent of its network status. Valid values are: • Disabled indicates that the resource is inoperable because of a fault, or it is not available. • Enabled indicates that the resource is operable and available for use. • Active indicates that the resource is operable and currently in use with operating capacity available to support further services. • Busy indicates the resource is operable and currently in use with n operating capacity to spare.
Physical Index	The given index associated to the resource. This is useful when a vital device component, such as a power supply or fan has sensors attached.
RTM Category	The resource's right-to-manage category.
Serial Number	The resource's serial number.
Service Tag	The device's service tag.
SupportAssist Status	The device's SupportAssist status. Valid values are Opt-In and Opt-Out.
System Object ID	The identifier for the resource's system object.
Topology Icon Size	The equipment icon size. Modify this size by right-clicking a device and then selecting Edit.

Pop-Up Menu

The Managed Resources pop-up menu provides access to the following options. Right-click a row to access these options.

Menu Option	Description
New	You can create a new device without discovering it with this menu item. Select the device vendor, model and type in the next screen, then fill in the information about the device in the editor that appears after that selection.
Edit	This lets you use the following screens: • Resource Editor: General • Resource Editor: Authentication • Resource Editor: Management Interface • Resource Editor: Custom Attributes—This tab appears only if you have configured custom attributes. See Redcell > Data Configuration on page 682 for more about them. Click *Save* to preserve any changes made in these screens to OpenManage Network Manager's database, or *Close* to abandon any changes made in editor screens. Unless the device is a printer, changes to these screens typically make database changes, not changes on the device. **Note:** You can edit fields like Notes and Description in subcomponent cards by right-clicking them in the resource tree.
Details (Click+Shift)	Opens a Details screen for the selected resource. This contains information like the performance indicators, power supplies and fans, monitor status summary, reference tree, network (ports, interfaces, details, and associated links), alarms and history events, audit train and execution history, performance data, and maintenance information.
Manage	Provides access to the following actions: • Set Management State for the selected devices to one of the following states: • Normal — The device is unconstrained by the other Administrative States. Changing from Suspended to Normal stops alarm suppression. Standard access, and inclusion in right-to-manage count. • Decommissioned — While this device is in inventory, it is not active. No device access allowed, no Monitor associations, no event processing, no Management Interfaces, no Authentication, no links, and no services are permitted. • Suspended — Suspends all device-related activities. No device access allowed, Monitoring Suspended, No event processing, Counts against right-to-manage. • Planned — The planned (future) device. No device access allowed, no monitor associations, and no event processing. • Maintenance — Neither alarms or polling apply to the device. Does allow resync and Adaptive CLI. Standard device visibility. The Management State menu option is available if the write permissions are functional. • Set Domain Access Control Select the Multitenancy domain where the selected device is to be visible, or manageable. This only appears if you implemented the Multitenancy option. Refer to the OpenManage Network Manager *Installation Guide* for details about that option. • View the Maintenance Log log for the selected device. See Connected Devices Portlet on page 538 for more about maintenance logging capabilities.

Menu Option	Description
Visualize	Displays a topology map that includes the selected resources. See Using Visualization Tools on page 143 for more about these maps.
Actions	Displays a list of action that you can initiate, such as Adaptive CLI Actions and other actions specific to the selected device. The list's content depends on the device selected. Use the magnifying glass search option to narrow the list of actions. Select an action and then click Load Selected to run it manually. See Actions Portlet on page 265 for more about configuring these activities.
Change Management	Executes or schedules for execution one of the following policies based on the option selected: • Change Determination runs the selected device. (See Change Determination Process on page 344.) • Execute Proscan runs any Proscan policies connected to the selected device. • Execute Proscan Policy runs any Proscan. (See Compliance Policy Summary on page 324.)
Direct Access	Open an SNMP Mib Browser to the alarmed device, a CLI Terminal (Telnet window) to the alarmed device, or ICMP Ping the device alarmed. Only those available appear in the subsequent menu.
Event Management	Suppresses or updates alarms related to the selected resource. The following event management options available are: • **Start Alarm Suppression** starts alarm suppression after you enter a description and then click Start. A Success/Failure confirmation message is displayed. • **Stop All Alarm Suppression** discontinues all alarm suppression. A confirmation message is displayed. You can also stop alarm suppression using the View Active Suppressions option. • **Schedule Alarm Suppression** opens the New Schedule *suppressionAction* window, where you set the exception options and suppression targets parameters and then set the schedule options. • **View Active Suppressions** displays a list of active suppressions. A messages is displayed if there are no active suppressions. You can stop selected alarm suppressions from this list. • **View Event History** shows event history for the selected resource in the Event History portlet. • **Resync Alarms** refreshes the information displayed with the latest information in the database for the selected resource or all resources. Except for View Event History, perform these actions on one or more resources.
File Management	Displays a current configuration file, compares it to previous backups, backs up, restores, imports or exports a configuration file by selecting the appropriate option. You can also deploy firmware to devices from this menu. If you go to the Configuration Files portlet, you can also edit backed up configuration files. See File Management Menu on page 582 for details.
Links	Create a new link or discover links between members of the selected group, and others. See New Link on page 532 and Link Discovery on page 533 for details.
Performance	Shows performance data for the selected interfaces in the Performance Dashboard window. Click the edit tool to modify the dashboard view properties, entities, or attributes. See Dashboard Editor on page 227 for more about the editor and its options.
Resource Groups	Adds the selected device to new Dynamic or Static groups, or to existing groups. See for Managed Resource Groups Portlet on page 637 more about this.

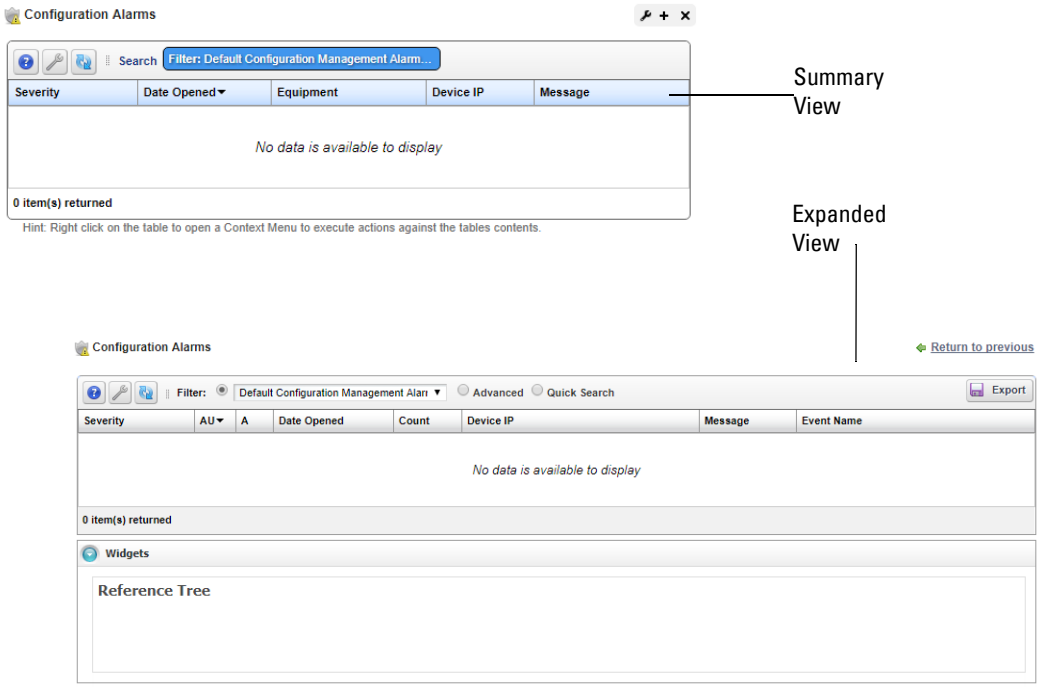
Menu Option	Description
Resync	Queries the device again for more current information, including alarms.
SupportAssist	Changes whether the selected devices SupportAssist status is Opt-In or Opt-Out. This option is available only if you have configured the Dell EMC SupportAssist feature.
Traffic Flow Analyzer	Configures the selected device to appear in the Traffic Flows displays when you select the Register option. Selecting UnRegister removes the selected device from the Traffic Flows displays. See Traffic Flow Analyzer on page 239 for more details on the analyzer. Show Traffic options display the traffic flow information for registered devices in an expanded Traffic Flow portlet. This displays Traffic Flow Analysis data that contains the endpoint for the selected device IP (if available) whether or not it is a registered exporter. You also have the option to execute or schedule execution for: • Create Configuration • Remove Configuration • Show Configuration
Delete	Removes the selected devices from inventory.
Edit Custom Attributes	Opens the Custom Attribute Editor where you define field characteristics, such as whether it is enabled, the label name, and the tooltip.
View as PDF	Creates an Acrobat PDF document containing the selected alarms' content displayed in the portlet.
Share with User	Opens the Share with User window where you select the colleague you want to share the selected alarms with and then type your message.

Configuration Alarms

Use the Configuration Alarms portlet to view alarms generated by a configuration action, such as backup, restore, or deploy and filter out those alarms not related to configuration actions. You can expand or change to event history to show all events.

This portlet is intended for users who are interested in managing the configuration of their discovered devices.

Access this portlet by selecting the Configuration Management page. This portlet has both a summary view and an expanded view. Each view displays different columns and have the same pop-up menu options available.



See Alarms in Visualizations/Topologies on page 530 to understand how alarms appear in the topology portlet.

Columns

Other than the general navigation and configuration options, the Configuration Alarms portlets (summary and expanded views) include the following columns. The columns displayed by default are noted.

You can view the value for most of the hidden columns by clicking the Settings tool, selecting the columns tab, clicking Show for the appropriate column, and then applying the change.

Column	Description
Severity	The alarm severity indicated by the color and text. The severity only has meaning for alarms and security alarms. Informational alarms have a severity level of Indeterminate. Closed alarms show without color. This field displays on the summary and expanded views by default.

Column	Description
Assigned User (AU)	The user currently assigned to this alarm. You can filters your assigned alarms using the Advanced filter option and selecting Assigned by User, contains, and entering your user ID. This field displays on the expanded view by default.
Acknowledged (A)	An indicator whether the alarm is acknowledged (checkmark) or not (X).
Date Opened	The date the alarm was created. This field displays on the summary and expanded views by default.
Count	The number of instances for this alarm. Multiples of the same alarm show as a single row but this value increments as more instances occur. This field displays on the expanded view by default.
Equipment	The entity emitting the alarm. This field displays on the summary view by default.
Device IP	The equipment IP address where the alarm appeared. This field displays on the summary and expanded views by default.
Message	The message associated with the alarm. This field displays on the summary and expanded views by default.
Event Name	The event associated with the alarm. This field displays on the expanded view by default.
Widgets	Additional information about the selected alarm, such as: • Reference Tree shows the connection between the alarm and its resource. • Alarm Details shows the severity, message, date opened, and so on. • MIB Details shows notification OID and MIB text. • Total Occurrences by Date shows a graph of the total occurrences by date. The Widgets field is available **only** from the expanded view.
The remaining field descriptions are available for use but do not appear on the default Configuration Alarms portlets.	
Date Cleared	The date and time the alarm was closed.
Update Date/Time	The time stamp for when the alarm was updated.
Date Assigned	The date and time that the alarm was assigned.
Assigned By	The user ID for the person that assigned this alert.
Ack Time	The time that the alarm was acknowledged.
Alarm State	The alarm's open or closed state.
Cleared By	The user ID for the person that cleared the alarm.
MIB Text	The alarm's MIB text.
Ack By	The user ID for the person that acknowledged the alarm.
Correlated By	The user ID for the person that cleared the alarm.
Correlated Time	The date and time when the alarm correlation to a parent alarm (caused by or blocked by).
Correlation State	The role the alarm plays in any correlation, such as top-level alarm, caused by parent, blocked by parent.
Domain	The domain emitting the alarm.
Entity Name	The entity emitting this alarm.
Entity Type	The type of monitored entity.
Has Children	An indicator that shows whether the alarm has children (checkmark) or not (X).

Column	Description
Highest Severity	The highest severity assigned to the selected alarm.
Include child alarms	An indicator that shows whether the alarm includes child alarms (checkmark) or not (X).
Location	The alarm's location.
Notification Type OID	The identifier for the notification displayed as an alarm.
Original Severity	The original severity specified for the selected alarm.
Parent Alarm	The name of the parent alarm.
Region	The alarm's region.
Resource Propagation	The propagation for this alarm, if any.
Service Affecting	Indicates whether the alarm is on equipment in a provisioned service (checkmark) or not (X). A service affecting alarm propagate to show as a component of service- and customer-related alarms. Service-Affecting alarms are of indeterminate or greater severity.
Service Propagation	The alarm propagation if Service Affecting is true in the event definition. This is similar to Resource Propagation, but controls **only** whether alarms affect services associated with entities hierarchically related to the alarmed entity. For example, if a port alarm is created and its event definition specifies that the Service Propagation is Impacts Subcomponents, then the alarm propagates only to the services associated with this port's interfaces. This does not affect the services associated with the top-level device.
Suppressed	An indicator whether the alarm is suppressed (checkmark) or not (X).
Suppression Date	The date and time of the alarm's suppression, if applicable.
Suppressor	The alarm that suppresses the selected alarm.

Pop-Up Menu

The Configuration Alarms pop-up menu provides access to the following options. Right-click a row to access these options.

Menu Option	Description
Edit	Opens the Edit Alarm window (see Alarm Editor on page 481) or the Editing Event Definition window (see Event Definition Editor on page 498).
Details (Click+Shift)	Opens a Details screen for the alarm itself, not the entity emitting it. (see Connected Devices Portlet on page 538 for an example of this type of screen). This contains information like the MIB text, any Event Processing Rules invoked, and a Reference Tree for the alarm. It also lets you configure alarm correlation. See Parent / Child Alarm Correlation: Alarm Details Panel on page 479. Select Alarm Details or Equipment Details
Visualize	Displays a topology map that includes the selected alarms. See Using Visualization Tools for more about these maps.
Acknowledge Alarm	Acknowledges the selected alarms. The current date and time appear in the Ack Time field. The checkmark appears in the expanded portlet for acknowledged alarms. This option is available when the selected alarms **are not** acknowledged.

Menu Option	Description
Unacknowledge Alarm	Unacknowledges previously acknowledged alarms, and clears the entries in the Ack By and Ack Time fields. When an alarm is not acknowledged, the red icon appears in the expanded portlet. This option is available when the selected alarms **are** acknowledged.
Assign User	Assigns selected alarms to one of the users displayed in the sub-menu by selecting that user. An icon also appears in the expanded portlet indicating the alarm is assigned to someone.
Clear Alarm	Removes the selected alarms from the default alarm view and marks them as a candidates for the database archiving process (DAP). Clearing alarms is an indication to the system that the alarms are resolved/addressed. If your system has propagation policies enabled, clearing recalculates dependent alarms.
Clear Group of Alarms	Removes a group of alarms from the default alarm view and marks them as candidates for DAP. This option is useful when you have many unimportant alarms that you want to clear at the same time instead of individually. For example, perhaps you want to clear all alarms that are informational and are more than a week old. Before selecting this menu item, create a filter for the group of alarms that you want to clear. When you select Clear Group of Alarms, a list of defined filters appears. Select the appropriate filter and then click Execute. All open alarms that meet the filter criteria are cleared. **Caution:** The Clear Group of Alarms action is irreversible.
Direct Access	Open an SNMP Mib Browser to the alarmed device, a CLI Terminal (Telnet window) to the alarmed device, or ICMP Ping the device alarmed. Only those available appear in the subsequent menu.
Email Alarm	Opens the Email Alarm window, where you specify a subject and e-mail address to which you want to mail the alarm's content, and then click Send Email. Click Cancel to end this operation without sending e-mail. SMTP setup is required to e-mail an alarm. See SMTP Configuration on page 626 for instructions about setting up e-mail from OpenManage Network Manager.
Show Performance	Shows performance data for the selected interfaces in the Performance Dashboard window. Click the edit tool to modify the dashboard view properties, entities, or attributes. See Dashboard Editor on page 227 for more about the editor and its options.
Aging Policy	This lets you select a policy that determines how long the selected alarms remain in the database. See Implementing DAP on page 38 for information about configuring such policies.
Edit Custom Attributes	Opens the Custom Attribute Editor where you define field characteristics, such as whether it is enabled, the label name, and the tooltip.
View as PDF	Creates an Acrobat PDF document containing the selected alarms' content displayed in the portlet.
Share with User	Opens the Share with User window where you select the colleague you want to share the selected alarms with and then type your message.

Configuration Management Schedule

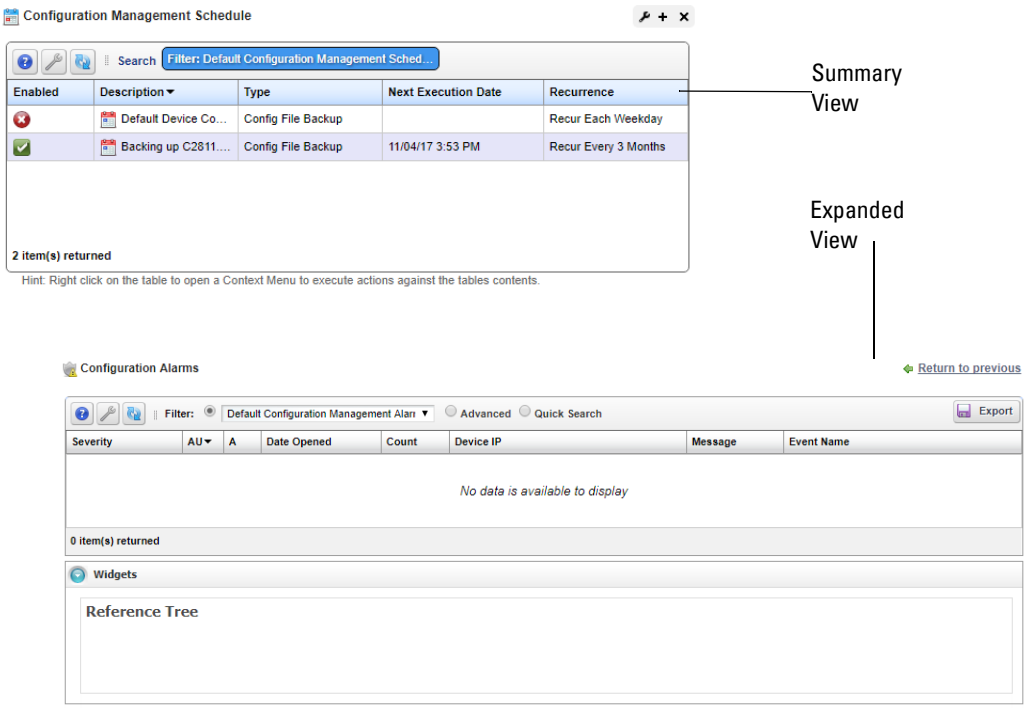
Use the Configuration Management Schedule portlet to quickly locate schedules pertaining to managed device configurations and to create and maintain schedules for the following action types:

- Config File Backup
- Config File Restore
- OS Image Deploy

The seeded Default Change Determination process backups a device if a configuration file change is detected. This runs agains all devices when turned on.

This portlet is intended for users who are interested in managing the configuration of their discovered devices.

Access this portlet by selecting the Configuration Management page. This portlet has both a summary view and an expanded view. Each view displays different columns and could have the same pop-up menu options available.



Columns

Other than the general navigation and configuration options, the Configuration Management Schedule portlets (summary and expanded views) includes the following columns. The columns displayed by default are noted.

You can view the value for most of the hidden columns by clicking the Settings tool, selecting the columns tab, clicking Show for the appropriate column, and then applying the change.

Column	Description
Enabled	An indicator that shows whether the schedule is enabled (checkmark) or not (X). This field displays on the summary and expanded views by default.
Description	The schedule description. This field displays on the summary and expanded views by default.
Type	The type of action scheduled, such as Config File Backup, Config File Restore, or OS Image Deploy. This field displays on the summary and expanded views by default.
Next Execution Date Recurrence	The frequency in which to execute the scheduled action, such as each weekday, every three months, only at startup, only once, and so on. This field displays on the summary and expanded views by default.
Submission Date	The date and time that this schedule was submitted. This field displays on the expanded view by default.
Start Date	The date and time to start the scheduled action execution. This field displays on the expanded view by default.
End Date	The date and time to end the scheduled action execution or the number of occurrences before ending this scheduled action. This field displays on the expanded view by default.
Finished	An indicator that shows whether the configuration execution completed (checkmark) or not (X). This field displays on the expanded view by default.
Execution Count	The number of times this scheduled action executed. Useful if you specified and end date based on the number of occurrences. This field displays on the expanded view by default.
Last Execution Date	The date and time that the action was executed. This field displays on the expanded view by default.
Domain ID	The Multitenant domain ID emitting the alarm.
Run Status	Indicated the schedules current state, such as waiting. Available to add to the summary/expanded view

Pop-Up Menu

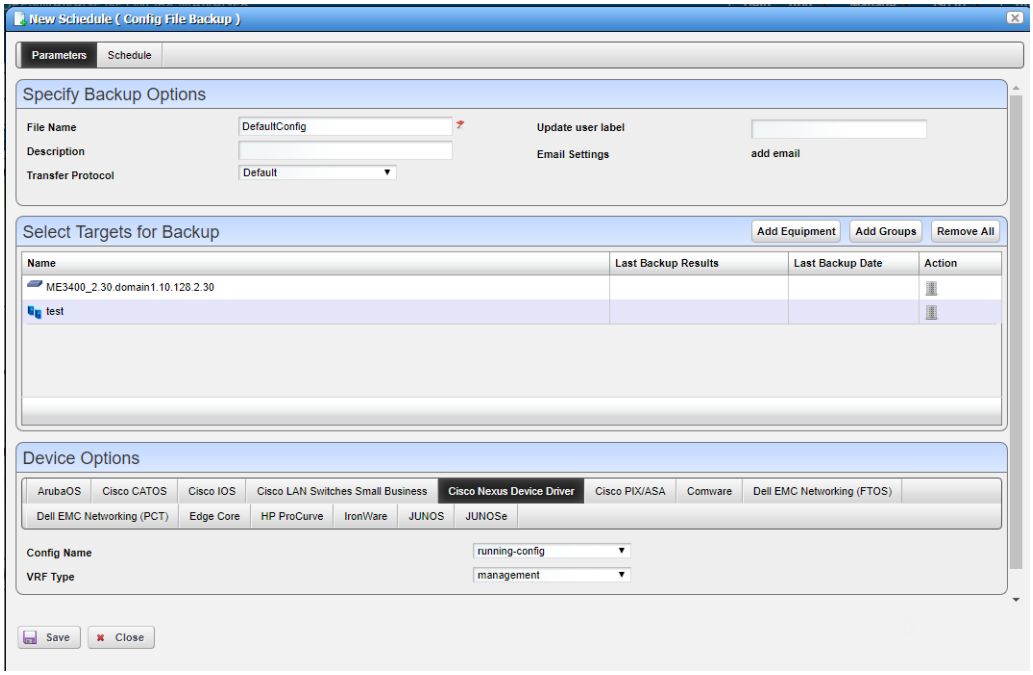
The Configuration Management Schedule pop-up menu provides access to the following options. Right-click a row to access these options.

Menu Option	Description
New	Provides access to the following schedule configuration types: • Config File Backup • Config File Restore • OS Image Deploy Once you select the configuration type, the New Schedule (*configType*) window opens, where you configure actions, their targets, and the order in which they execute. You can also create a schedule from a portlet that ordinarily executes them using the Schedule option. For example Discovering Resources on page 138.
Edit	Opens the Editing Schedule (*configType*) window, where you modify the selected schedule's settings. This option appears for activity-based configurations. You can also edit a schedule from a portlet that ordinarily executes them using the Schedule option. For example Discovering Resources on page 138.
Delete	Deletes the selected schedule configuration. A confirmation message is displayed. Click Delete to continue with the deletion. Click Cancel to disregard the request.
Enable Schedule	Activates the selected schedule. This option appears if the selected schedule is disabled. You can also enable a schedule using the Edit option and selecting the Enabled option.
Disable Schedule	Deactivates the selected schedule. This option appears if the selected schedule is enabled.
Execute	Runs the scheduled action. If the scheduled action is activity-based or discovery-profile-based, an audit viewer appears progress of the selected item. For other scheduled action types, a message is displayed sating that the scheduled items were sent to the application server for immediate execution. Use the Audit Trail portlet to monitor progress (see Audit Trail Portlet on page 630) for details.
Share with User	Shares selected alarms with other colleagues on your OpenManage Network Manager system, and consults with them using the conferencing feature.

Config File Backup

Use the New Schedule (Config File Backup) window to specify the backup options, targets for backup, device options, and then schedule the backup.

Access this window by right-clicking a configuration and then selecting New > Config File Backup.



The Config File Backup Parameters window has the following fields and options. See Schedule on page 671 for scheduling fields and options descriptions.

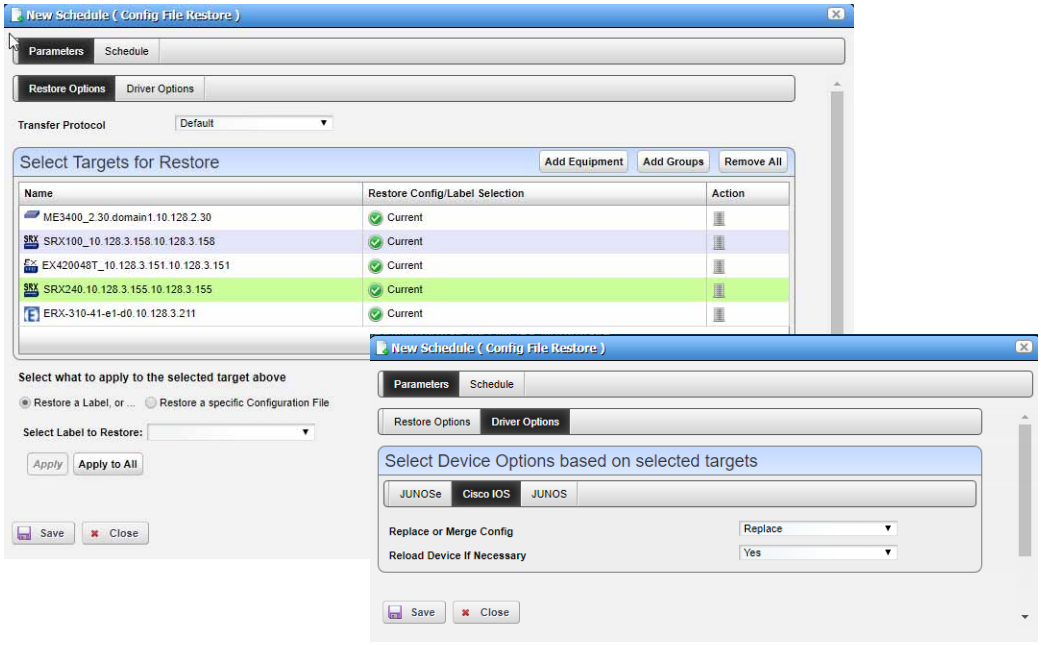
Field/Option	Description
File Name	This name is used as the backed up configuration file during server transfers and saved in source control. The backed up configuration file will be name this during the server transfers and saved in the source control. Due to limitations of some devices, do not exceed 15 characters for the filename.
Description	Provides a description of the file as it's checked into storage.
Transfer Protocol	Specifies which protocol is used (Default, FTP, TFTP, or SFTP) to transfer files.
Update user label	Creates or points the selected user label to the backed up configuration file.
Email Settings	Opens a window where you specify email options and recipients.
Add Equipment	Adds the selected equipment to the Targets for Backup list.
Add Groups	Adds groups of devices to the Targets for Backup list.
Remove All	Deletes all devices and groups from the Targets for Backup list.
Targets for Backup	Provides the following information for each target: • Name • Last Backup Results • Last Backup Date • Action deletes the entry

Field/Option	Description
Device Options	Lists the tabs for each device based on your target backup list. Click a device tab to view its options, such as Config Name, VRF Type, Config File, Configuration Type, on so on.

Config File Restore

Use the Config File Restore window to specify the targets for restore, device options for the selected targets, and schedule the restore.

Access this window by right-clicking a configuration and then selecting New > Config File Restore.



The Config File Backup Parameters panes has the following restore and driver fields and options. See Schedule on page 671 for scheduling fields and options descriptions.

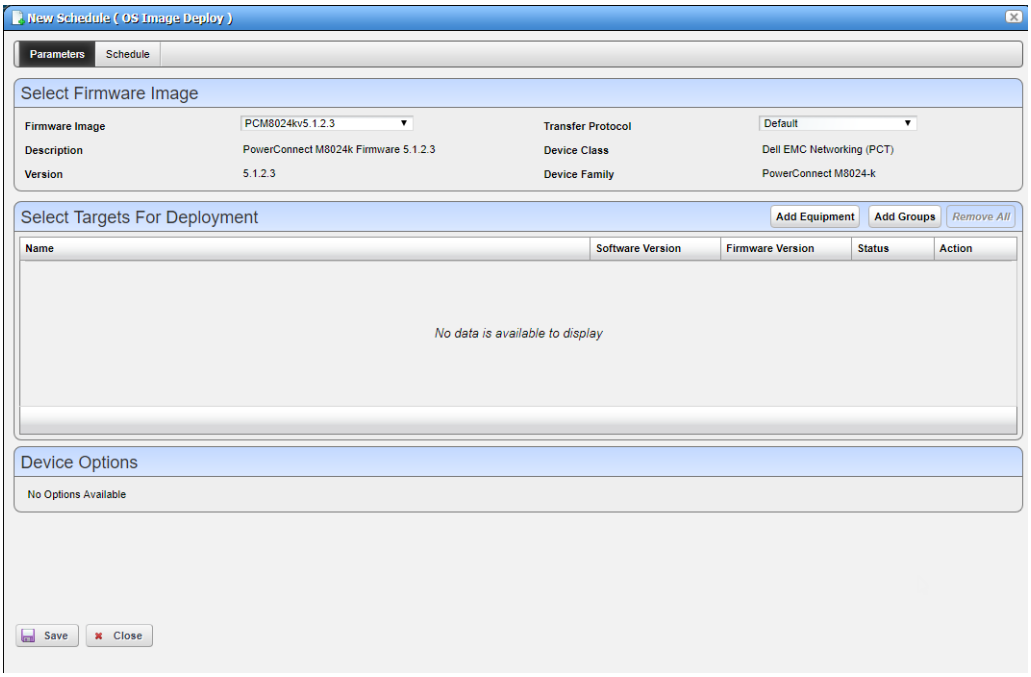
Field/Option	Description
Transfer Protocol	Specifies which protocol is used (Default, FTP, TFTP, or SFTP) to transfer files.
Add Equipment	Adds the selected equipment to the Targets for Restore list.
Add Groups	Adds groups of devices to the Targets for Restore list.
Remove All	Deletes all devices and groups from the Targets for Restore list.
Targets for Restore	Provides the following information for each target: • Name • Restore Config/Label Selection • Action deletes the entry When you select to target to restore, the following options appear: • Restore a Label • Restore a specific Configuration File. If you select Restore a Label, select a label to restore. If you select Restore a specific Configuration File, select the configuration file from the list.

Field/Option	Description
Device Options	Lists the tabs for each device based on the restore target selected. Click a device tab to view its options, such as Replace or Merge Config, Reload Device If Necessary, Load Action, on so on. Select the appropriate action for each option.

OS Image Deploy

Use the OS Image Deploy window to specify firmware image, targets for deployment, device options, and then schedule the OS image deployment.

Access this window by right-clicking a configuration and then selecting New > OS Image Deploy.



The OS Image Deploy Parameters window has the following fields and options. See Schedule on page 671 for scheduling fields and options descriptions.

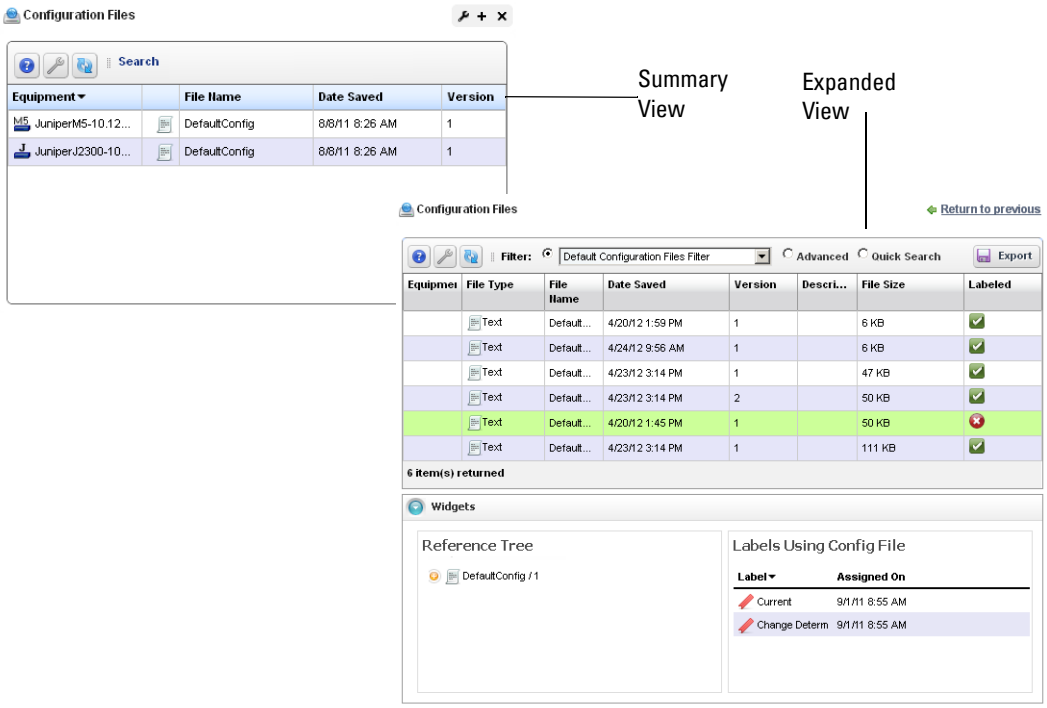
Field/Option	Description
Firmware Image	Specifies which image you want to deploy.
Description	Displays the selected firmware image description.
Version	Displays the selected firmware image version.
Transfer Protocol	Specifies which protocol is used (Default, FTP, TFTP, or SFTP) to transfer files.
Device Class	Displays the selected firmware's device class.
Device Family	Displays the selected firmware's device family.
Add Equipment	Adds the selected equipment to the Targets for Deployment list.
Add Groups	Adds groups of devices to the Targets for Deployment list.
Remove All	Deletes all devices and groups from the Targets for Deployment list.

Field/Option	Description
Targets for Deployment	Provides the following information for each target: • Name • Software Version • Firmware Version • Status • Action deletes the entry
Device Options	Lists the tabs for each device based on the deploy target selected. Click a device tab to view its options. Select the appropriate action for each option.

Configuration Files Portlet

Use the Configuration Files portlet to view backed up configuration files. To see the most recent configuration files, see Top Configuration Backups on page 222.

Access this portlet from the Configuration Management page. This portlet has both a summary view and an expanded view. Each view could display different columns and has the same pop-up menu options available.



Columns

Other than the general navigation and configuration options, the Configuration Files portlet includes the following columns. The columns displayed by default are noted.

You can view the value for most of the hidden columns by clicking the Settings tool, selecting the columns tab, clicking Show for the appropriate column, and then applying the change.

Column	Description
Equipment	The equipment impacted by the configuration. This field displays on the summary and expanded views by default.
File Name	A descriptive name given to the configuration. This field displays on the summary and expanded views by default.
Date Saved	The date and time the configuration file was saved. This field displays on the summary and expanded views by default.
Version	The version for the selected configuration. This field displays on the summary and expanded views by default.
File Type	The type of file in which the configuration is stored, such as text. This field displays on the expanded view by default.
Description	A detailed description for the configuration. This field displays on the expanded view by default.
File Size	The configuration file size (KB/MB). The OMNM system converts from bytes to KB/MB and presents the file size in terms of KB/MB after some rounding. For example, 1484 bytes/1024 = 1.44921875 KB, which is rounded to 1.45 KB by the OMNM system. In an advanced search by file size, search for a range to accommodate the rounding conversion. This field displays on the expanded view by default.
Labeled	An indicator that shows whether the configuration file has a label (checkmark) or not (X). When a configuration has a label applied, you cannot delete or archive it. This field displays on the expanded view by default.
Widgets	Additional information about the selected image, such as: • Reference Tree shows the configuration file name and provides access to the operations it supports by right-clicking the file name. • Labels connected to the selected configuration file and the date on which the connection was made. The Widgets field is available **only** from the expanded view.

Pop-Up Menu

The Configuration File pop-up menu provides access to the following options. Right-click a row to access these options.

Menu Option	Description
View	Opens the Configuration File editor, where you can see the configuration file content if it is a non-binary file.
Edit	Opens the Configuration File editor, where you can edit the backed up, non-binary configuration file. See File Management Menu on page 582 and Configuration File Editor on page 585 for a description of these capabilities.
Assign Labels	Labels a single selected configuration file. A label selector appears that lets you select an existing label and create a new one. If you assign one file the Current label, others from the same device cannot have it. OpenManage Network Manager automates moving Current from one file to the other, if another has it. You can delete non-system labels from devices in the selector this menu item produces.
Compare to Label/ Compare Selected	Compares labeled configuration files to the current selection. See File Management Menu on page 582 for a description of this capability. You can create labels when you back up a config file, or you can compare to the default labels (Change Determination, Current, Compliant). If you select two configuration files in the expanded portlet, you can also Compare Selected.
Promote	Makes the selected configuration file available for mass deployment. This is a useful way to make a **pattern** configuration file to deploy to several devices. See Configuration on page 590 for additional information about how to do this.
Backup/Restore	Backs up the device (again) related to the selected file, or restores the selected file to its device. **Note:** The OpenManage Network Manager system automatically assigns the most recently restored file the *Current* label.
Archive	Saves the selected file to disk, and optionally deletes it from this list.
Import/Export	Export the selected config file to disk, or import it from disk. You can also import/ export a selected configuration file. Provides the following actions when available for the selected image: • Import retrieves a file containing XML compliance descriptions. Some imports can come from a URL. • Export Selection exports the selected description to an XML file. • Export All exports all descriptions to an XML file. Click Download Export File to specify where to save the file. The Import/Export option is useful as a backup or to share descriptors with other projects. You must import data into the correct portlet. For example, you cannot import event data into the Actions portlet. If one type of data depends on another, you must import the other data before importing the data that depends on it.
Delete	Removes the file from the OpenManage Network Manager database without exporting it.
Aging Policy	Opens the Aging Policy selector., where you specify how long this file remains in the database. See Implementing DAP on page 38 for more about about configuring such policies.
Share with User	Opens the Share with User window where you select the colleague you want to share this asset with and then type your message.

File Management Menu

In addition to letting you back up and restore configuration files, and deploy firmware updates to devices, this menu manages viewing and comparing configuration files backed up from the selected devices. Details about these capabilities appear below.

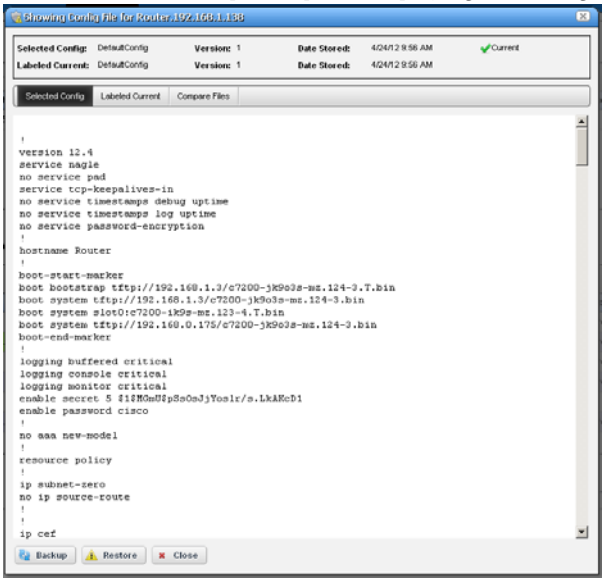
Compare and *View* options have the following limitations:

- If you select a config file that is a single file, without any historical precedent, no comparison option appears on the menu since the selected version does not have a prior version.
- If you select a single config file of version two or higher, comparison is an option. When selected, OpenManage Network Manager automatically compares against the most recent prior version for that device and file name.
- If you select two config files of any version, OpenManage Network Manager compares those two versions.
- If you select three or more config files, no comparison option appears.
- The *View* option appears for a single selection only, and only lets you view files that are not binary.

The icon to the left of the *File Name* listed in the portlet lets you know whether a configuration file is binary ( ), and not viewable, or text ( ), and viewable.

The file management menu contains the following:

View / Edit — This opens a panel displaying the configuration file's contents. Use the browser's



Find function (as demonstrated on the right) to locate specific text within the Config File. You can also select and copy text within this screen.

Notice that *Selected Config* and *Live Config* (current) version and storage dates appear at the top of this screen. When you perform a backup that differs from the config that is *Labeled Current*, that label changes to *Live Config* if changes are detected.

Selected Config appears when you open this screen from the Configuration Files Portlet Portlet, but *Live Config / Current Config* appear side-by-side when you open this screen from the Managed Resources portlet.

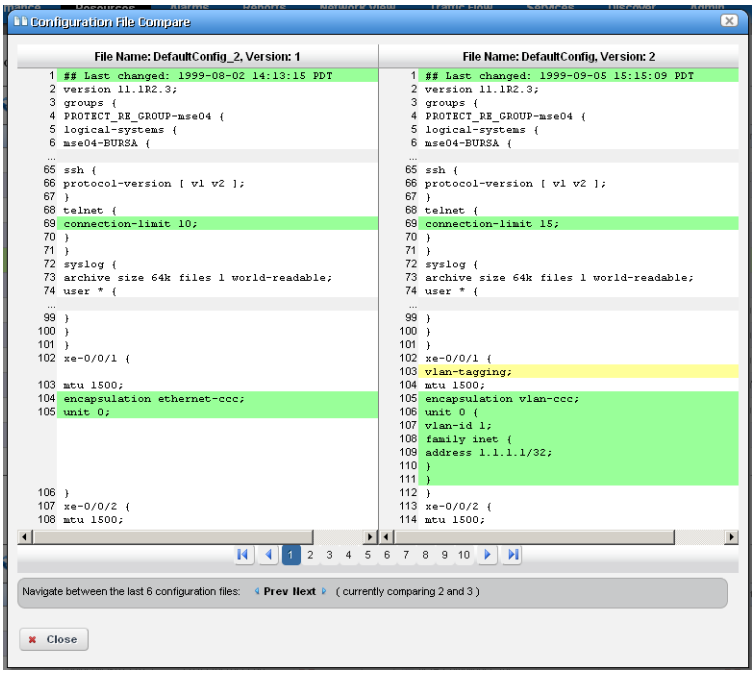
You can also compare two different configurations (*Selected Config* and *Labeled Current / Live Config*) in the tabs that appear on this screen. with the *Compare Files* tab at the top.

Close the screen with the buttons at its bottom. Notice you can also *Backup* or *Restore* what you are viewing with buttons at the bottom of the screen.

Assign Labels—Use this option to select an existing label or create a new one. You cannot assign System labels (*Current*, *Compliant*, and so on).

Compare Current v. Previous / to Label / Selected—You can compare configurations by right-clicking a device, or two devices then selecting *Compare*. If you right click a single device with a previous backup, then the comparison is between the latest and next-to-latest backup. If it does not have a previous backup, then the menu offers to compare to a designated label. You can compare two different *Selected* devices too. Ctrl+click to select two different devices before you *Compare*.

Notice that the *Prev / Next* buttons at the bottom of this screen can cycle through as many as



five previous configuration files.

The comparison screen appears with the configurations side-by-side (note the file names in the title bar of this screen).

NOTE:

Colors: Lines that differ between the two configurations appear highlighted green. Lines missing in one, but that appear in another appear highlighted red. Added lines are yellow.

Use the right/left arrows to page through the side-by-side comparison. The page numbers and beginning / forward / back / end arrows help you navigate between pages of pairs of files. Notice also that if you have more than two such files, a panel appears at the bottom that lets you

navigate between adjacent pairs of such files (1 and 2, 2 and 3, 3 and 4, and so on). Click the Prev / Next links to move between pairs of files.

NOTICE

Use the browser's "Find" function (Ctrl+F) to locate text within these views.

Backup / Restore—Select these to backup or restore a configuration file. See Backing Up Configurations on page 151 or Restoring Configurations on page 152 for step-by-step instructions.

NOTE:

Some devices merge rather than replace configurations when you select Restore. (Cisco XR, for one)

Deploy—Select this option to deploy an OS Image (firmware). See Deploying Firmware on page 154 for more.

Some devices, including the Dell EMC Networking FTOS C-Series and E-Series, first permit then drop telnet connections during deployment or file restoration when you select restart as part of the process. This can take from six to eight minutes, though it can take as long as fifteen minutes for a fully populated chassis. During that time, ping detects the device; however, OpenManage Network Manager cannot log in to the device until the reboot is complete.

Restoring configurations to Dell Force 10 devices may produce errors when individual commands already exist in the running config and cannot be overwritten. OpenManage Network Manager ignores such errors and reports success by default since the errors indicate a command was not applied, not that restoration was unsuccessful. Best practice is to restore to startup config to avoid these errors, especially when scheduling backup or backing up a group on such devices.

NOTICE

"Console Logging" must be turned off on all devices.The messages from console logging interfere with the communication between OMNM and the device (via CLI) and can disrupt supported functionality in OMNM.

Export / Import —Export lets you save a local copy of the selected config file. Import opens a screen that lets you select a locally-accessible file to store, view, compare and deploy.

View configuration files in the *History* > *Latest Configurations* portion of the Connected Devices Portlet for a device or in the Configuration Files Portlet or Top Configuration Backups portlets.

Configuration File Editor

Use the Configuration File editor to manually edit configuration files, and save them to the OpenManage Network Manager database. You can edit only non-binary configuration files.

When you select a file from the Configuration Files Portlet portlet, and then right-click to select Edit, the Configuration File editor opens with the Find/Replace options.

Click the magnifying glass to open the text search feature. Select `A/a` to make your search case-sensitive, or `RegEx` to use regular expressions to search.

Click the Find button to locate text in the config file. Click Replace to replace the text found. Select All and then click Replace to globally replace all instances of the text found within the configuration file.

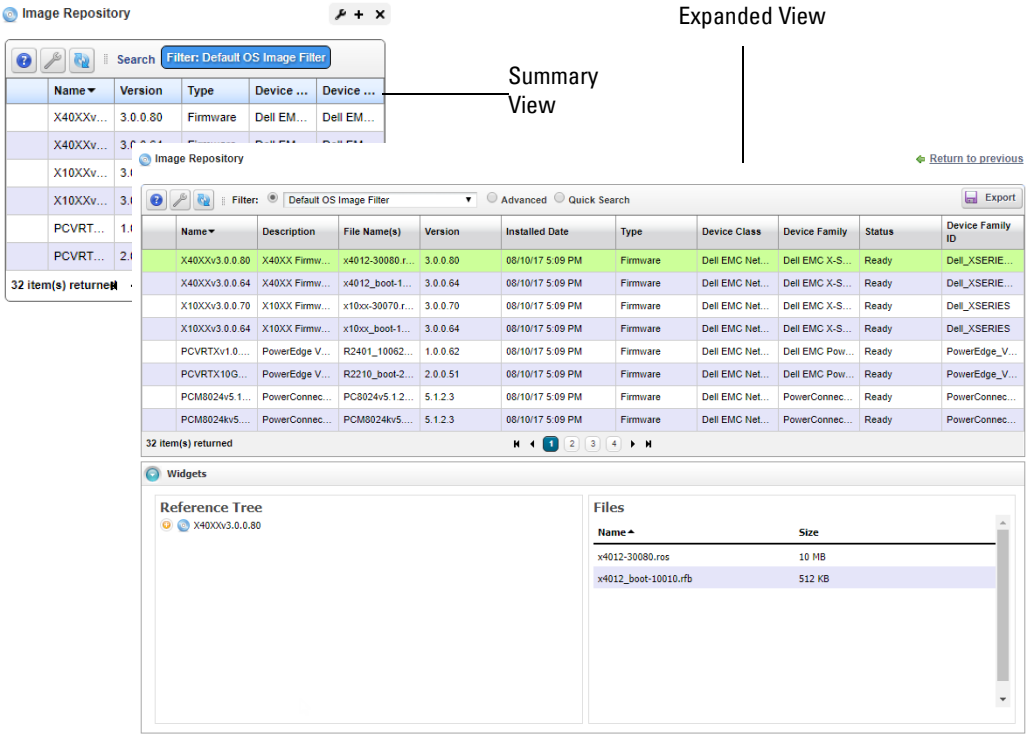
Click Save to preserve your edits, or Close to abandon them. Notice that the edited configuration is listed with the other Configuration Files in the portlet as a different version than the original. The version increments by one every time you edit and save a configuration.

Image Repository Portlet

Use the Image Repository portlet to manage firmware updates to deploy to devices in your network, or manage configurations that you want to deploy to several devices. Add these files to your OpenManage Network Manager system before deploying them.

This portlet is intended for users who are interested in managing firmware updates deployed to devices or manage configurations deployed to several devices.

Access this portlet from the Configuration Management page. This portlet has both a summary view and an expanded view. Each view could display different columns and has the same pop-up menu options available.



Columns

Other than the general navigation and configuration options, the Image Repository portlet includes the following columns. The columns displayed by default are noted.

You can view the value for most of the hidden columns by clicking the Settings tool, selecting the columns tab, clicking Show for the appropriate column, and then applying the change.

Column	Description
Name	The image name. This field displays on the summary and expanded views by default.
Version	The version for the selected image. This field displays on the summary and expanded views by default.
Type	The type of image, such as firmware, configuration, and so on. This field displays on the summary and expanded views by default.

Column	Description
Device Class	The device class for the selected image. This field displays on the summary and expanded views by default.
Device Family	The device family for the selected image. This field displays on the summary and expanded views by default.
Description	More details about the firmware or configuration. This field displays on the expanded view by default.
File Names	The files related to the selected image. These files are also listed in the Widgets field. This field displays on the expanded view by default.
Installed Date	The date and time in which the firmware was installed. This field displays on the expanded view by default.
Status	The device's readiness to deploy (failed, importing, ready). This field displays on the expanded view by default.
Device Family ID	The family of models for which the image works. This field displays on the expanded view by default.
Widgets	Additional information about the selected image, such as: • Reference Tree shows the connection between the image and its device. • Related files. Also listed in the File Names field. The Widgets field is available **only** from the expanded view.

Pop-Up Menu

The Image Repository pop-up menu provides access to the following options. Right-click a row to access these options.

Menu Option	Description
New	Opens the Firmware Image Editor window or the Configuration Image Editor window, where you define a firmware image or configuration, respectively.
Edit	Opens the Firmware Image Editor or the Configuration Image Editor if the selected line is a configuration image.
Deploy	Opens the Deploy Firmware window, where you define deployment options for the selected image. For this to function, you must enable a server. See File Management Menu on page 582 for details.
Download Firmware For	Downloads firmware from the internet for the selected device. The devices that support downloading (such as Dell DNOS or Dell FTOS) are listed as an option to the Download Firmware For menu option. Select the device for which you want to download OS images and the OpenManage Network Manager system automatically downloads it.
Delete	Removes the selected OS image or configuration from the list.
Share with User	Opens the Share with User window where you select the colleague you want to share this asset with and then type your message.

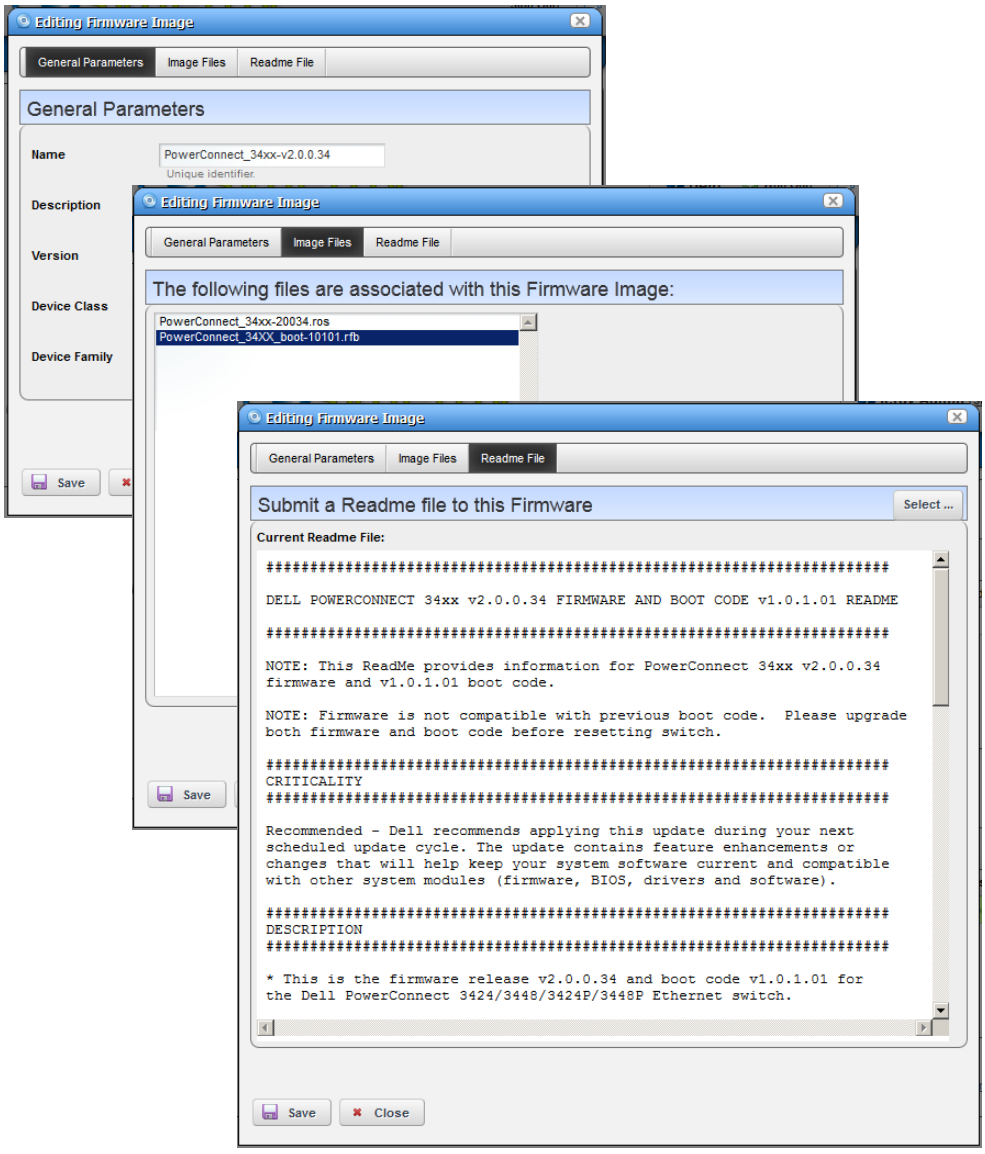
Firmware Image Editor

Use the Firmware Image editor to create or maintain OS images. This editor has the following panels:

- General Parameters specifies the general parameters, such as name, version, class, and so on
- Image Files specifies or displays image-related files
- Readme File to view or specify a text file related to the image

Click *Save* to preserve the OS Image you have configured, or *Cancel* to exit these screens without saving.

Access this editor from the Image Repository portlet by selecting the New > Firmware Image pop-up menu option or selecting a firmware image and then the Edit pop-up menu option.



The Firmware Image editor has the following fields or options.

Field/Option	Description
Name	Specifies a user-defined name for the image.
Description	Provides more details about the image.
Version	Provides a descriptive version number.
Device Class	Lists the available device firmware classes from which to choose. Based on the device class selected, the Device Family list is populated.
Device Family	Lists the device families available for the selected Device Class.
Image Files	Imports a file from disk or from URL when you create an image. Displays imported files when editing and image. Because OS images can consist of multiple files, you can import multiple files here.
Readme File	Imports a read me text file to accompany the image or displays the imported file content.

Configuration Image Editor

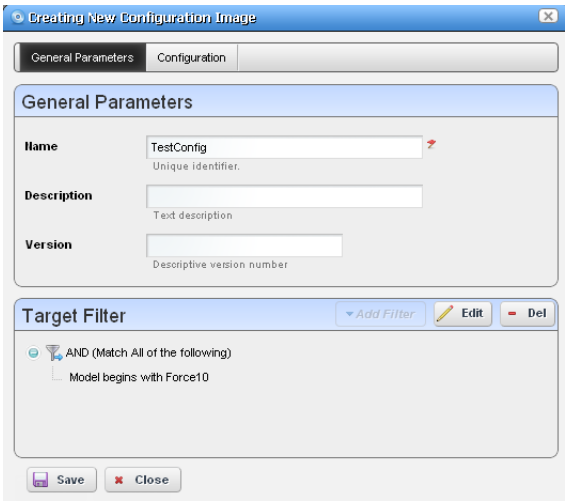
Use the Configuration Image editor to create and maintain image configurations. This editor has the following panels:

- General Parameters
- Configuration

Access this editor from the Image Repository portlet by selecting the New > Configuration Image pop-up menu option or by selecting a configuration image and then the Edit pop-up menu.

General Parameters

Use the General Parameters panel to name and describe the configuration file, and configure a filter to screen restoration targets.



The Configuration Image editor has the following fields or options.

Fields/Options	Description
Name	Specifies a unique identifier for the image configuration.
Description	Provides more details on the image configuration.

Fields/Options	Description
Version	Automatically tracks changes to the original.
Target Filter	Defines which devices to target. When targets fail, restoration skips them. Add filters by creating a filter or copying and existing filter.

Configuration

Use the Configuration panel to configure what is restored, and what is variable in mass deployments. Initially the configuration document is empty if you are creating a configuration image. However, it displays data from any promoted configuration file if it originated as a promoted configuration file.

Access this information by clicking the Configuration Image editor Configuration tab.

The Target Params list includes all available discoverable parameters. These parameters are stored in the OpenManage Network Manager database. Some parameters may not apply to a specific device or configuration file. To insert a parameter into the document, double-click it. If you are adding a parameter to an existing document, make sure that you indicate where you want to add it before double-clicking the parameter.

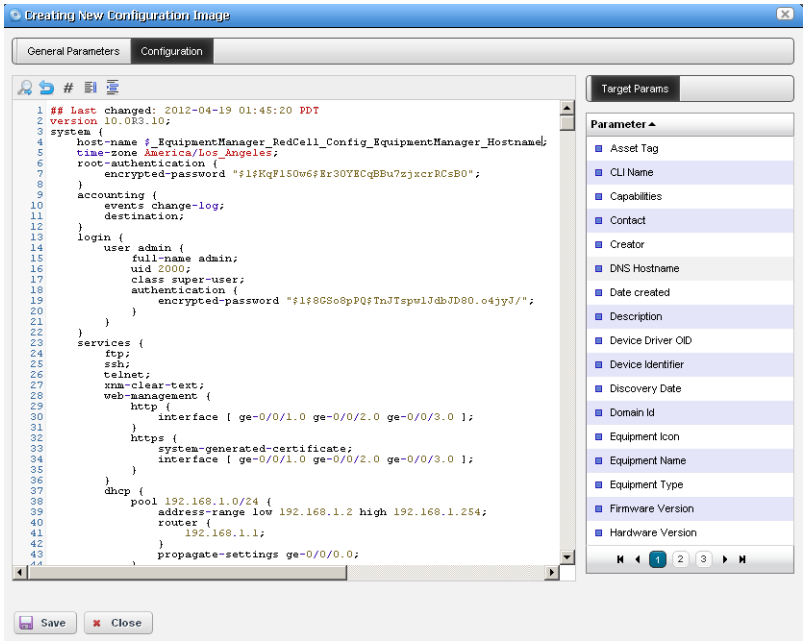
For example, if a Contact parameter appears in the configuration file, delete the specifics retrieved from a particular device's configuration and then double-click the Contact target parameter. The following line is inserted into the document where you put the cursor:

```
$_EquipmentManager_RedCell_Config_EquipmentManager_Contact
```

When you deploy this configuration file to the devices that pass the General Parameters target filter, the OpenManage Network Manager system updates this parameter with discovered data retrieved from the device before restoring the configuration. This facilitates deploying the same configuration to many devices while retaining individual target parameters like Contacts, DNS Hostname, and so on.

NOTICE

If you want to compare different promoted configuration file templates for the same devices, deploy both template #1 and template #2, then compare them in the Configuration Files Portlet on page 579 portlet. By default the Description notes that such configuration files are "Created from template."



Deploy Firmware

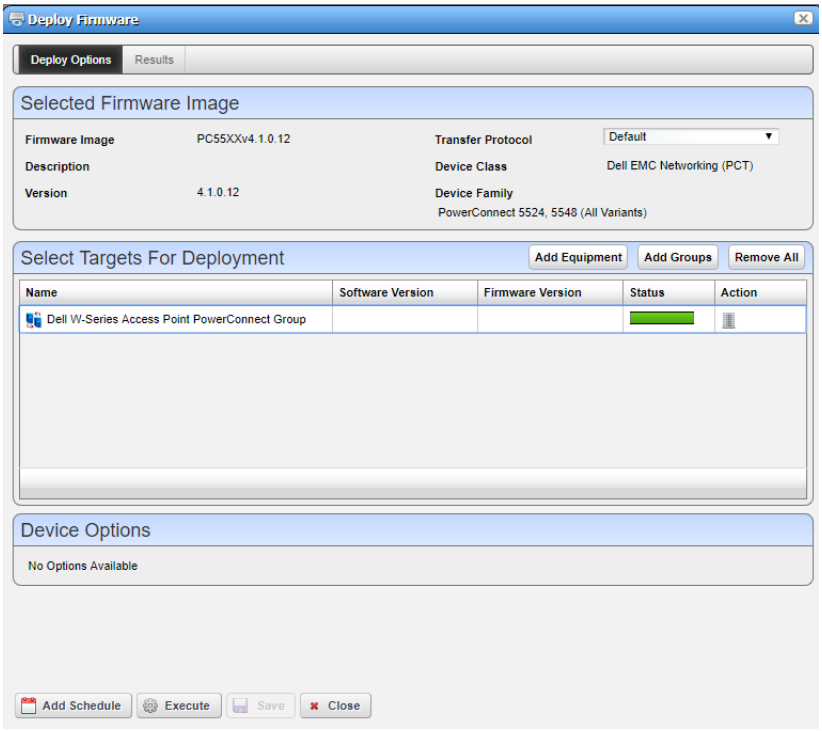
Use the Deploy Firmware window to configure a deployment, whether triggered from resource groups, individual resources, or the Image Repository Portlet portlet. Deployment validates that the selected image is appropriate for the selected devices, or appropriate devices within a group.

You have the option to select a transfer protocol, add target equipment or groups, execute immediately, or schedule the deployment for a later date/time. If you create a deployment schedule, save your configuration. Otherwise, close the window to abandon your edits.

NOTE:

When you add firmware to the Image Repository for Dell 35xx and 55xx devices, you must add both the boot image and firmware image together to deploy to these devices.

You may see multiple options for selecting the configuration file to backup for PowerConnect (not Dell EMC Networking FTOS) devices. Layer 2 Powerconnect switches have just running and startup options while the Layer 3 router has running, startup and backup options, so different options appear for the two sets of switches. When you do file backup for a group of devices, all those options are combined. Select only the top entry selection for execution.

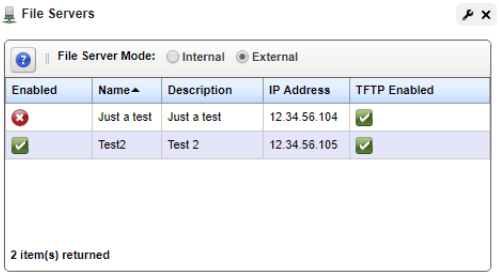


File Servers Portlet

Use the File Servers portlet to define and maintain a list of internal and external file servers. This portlet has only the summary view.

This portlet is intended for anyone that want to define and maintain file servers and they have the permission to do so.

Access this portlet from the Configuration Management page. This portlet has only a summary view with all columns showing and pop-up menu options available.



Columns

Other than the general navigation and configuration options, the File Servers portlet includes the following columns. All columns are displayed by default and there is not option to change the columns show.

Column/Option	Description
File Server Mode	An option to specify whether the file server is internal or external. The default is External.
Enabled	An indicator that shows whether the server is enabled (checkmark) or not (X).
Name	The user-defined name for the server.
Description	A detailed description for the server.
IP Address	The IP address used by the application.
TFTP Enabled	An indicator that shows whether the server supports TFTP (checkmark) or not (X).

Pop-Up Menu

The File Servers pop-up menu provides access to the following options. Right-click a row to access these options.

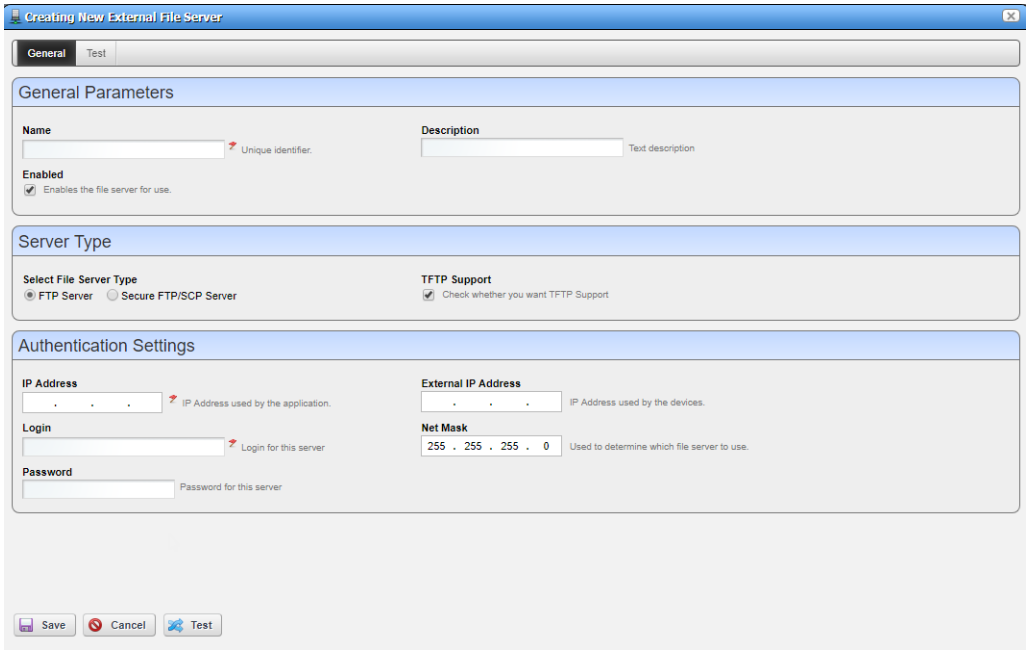
Menu Option	Description
New	Opens the External File Server editor, where you define an external file server by setting general parameters, specify server type (FTP, FTP/SCP) and whether you want TFTP support, and the authentication settings.
Edit	Opens the External File Server editor, where you modify the selected external file server's general parameters, server type (FTP, FTP/SCP) and whether you want TFTP support, and the authentication settings.
Disable	Disables the selected file servers from the list. A successful/failed message is displayed. This option shows only if the selected file servers are enabled.

Menu Option	Description
Enable	Disables the selected file servers from the list. A successful/failed message is displayed. This option shows only if the selected file servers are not enabled.
Test	Verifies your settings for the selected file server. Shows the test progress and the results in the Job Status window.
Delete	Removes the selected file servers from the list. A confirmation message is displayed. Click Delete to remove.
Share with User	Opens the Share with User window where you select the colleague you want to share this asset with and then type your message.

External File Server

Use the External File Server editor to define and maintain external file servers.

Access this editor by right-clicking the File Servers portlet and then selecting New, or by right-clicking and existing file server definition and then selecting Edit.



The External File Server editor has the following fields and options.

Field/Option	Description
Name	Is a unique name for the file server.
Description	Provides a detailed description for the file server.
Enabled	Activates the file server for use. Selected by default.
Server Type	Specifies one of the following file server types: • FTP Server (default) • Secure FTP/SCP Server **Note:** Secure FTP connections (scp/sftp) often require SSH services be enabled on the devices addressed. Make sure that your system's server and sftp/scp file server can also access the devices with SSH.

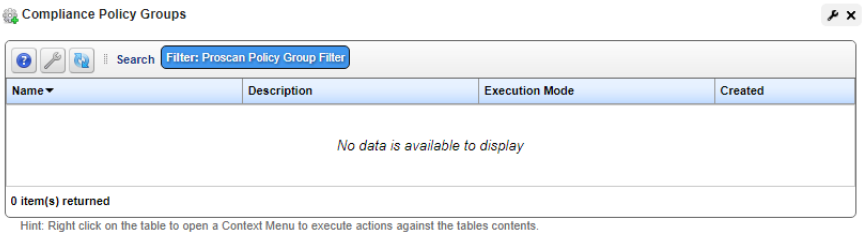
Field/Option	Description
TFTP Support	Indicates whether you want TFTP support. The default is to have TFTP support (selected).
IP Address	Specifies the IP address used by the application. This address is required.
External IP Address	Specifies the IP address used by the devices.
Login	Specifies the login defined for this server. This is required.
Net Mask	Determines which file server to use. The default is 255.255.255.0. If you have several servers, the specified net mask determises which server communicates with devices in which portion of the network.
Password	Specifies the optional password for the login name.
Test (panel)	Shows the Job Status and whether the test was successful or failed. Click the Test button to verify your file server configuration.

Compliance Policy Groups

Use the Compliance Policy Groups portlet to create and manage compliance policy groups. This portlet has only the summary view.

This portlet is intended for users who are interested in configuring and maintaining compliance policy groups.

Access this portlet from the Configuration Management > Compliance navigation bar. This portlet has both a summary view and an expanded view. Each view could display different columns and has the same pop-up menu options available.



Columns

Other than the general navigation and configuration options, the Compliance Policy Groups portlet includes the following columns. The columns displayed by default are noted.

You can view the value for most of the hidden columns by clicking the Settings tool, selecting the columns tab, clicking Show for the appropriate column, and then applying the change.

Columns	Description
Name	This information displays by default. This field displays on the summary by default.
Description	A more detailed description of the named group. This information displays by default.
Execution Mode	An indicator that the execution is internal or external. This information displays by default.
Created	The date that this group was created. This information displays by default.

Columns	Description
Domain	The domain where the policy resides.
Updated	The date that this group was updated.

Pop-Up Menu

The Compliance Policy Groups pop-up menu provides access to the following options. Right-click a row to access these options.

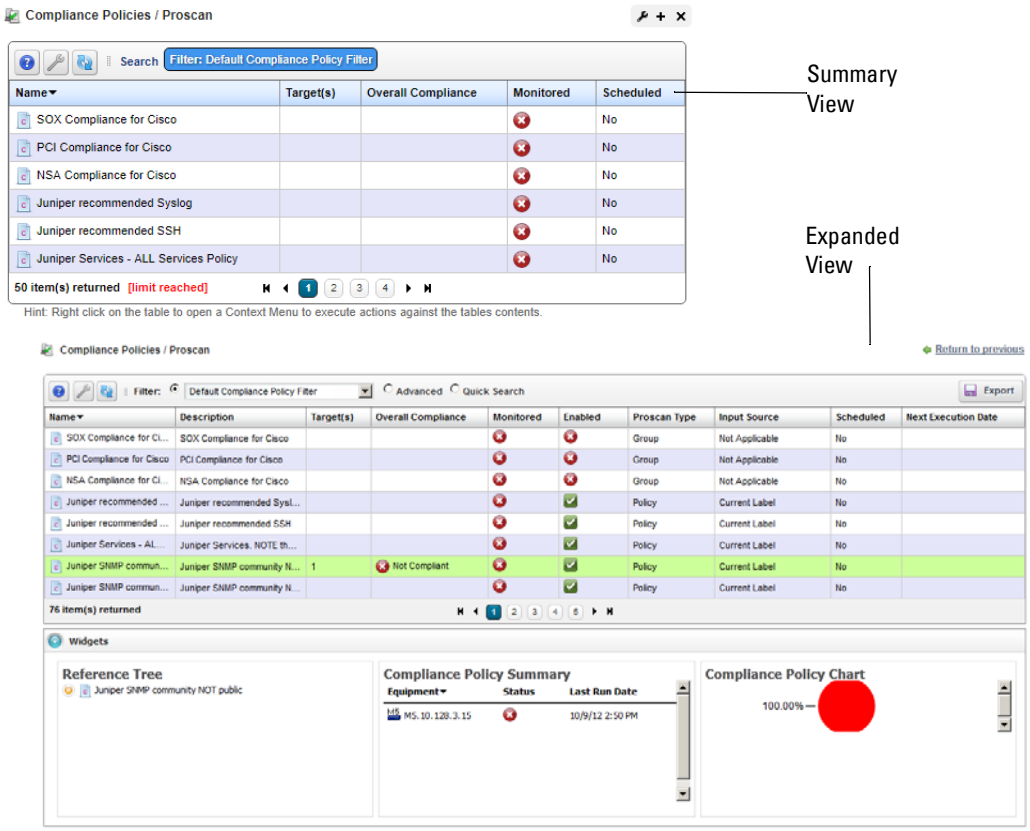
Menu Option	Description
New	Opens the Creating Action Group window, where you define a group action by selecting actions, providing a description, adding associated targets, and then defining parameters based on the selected actions and targets. See Action Group Editor on page 315 for more details.
Edit	Opens the Editing Action Group window, where you modify the general settings, actions, and/or edit a schedule.
Execute	Runs the selected policy.
Audit	Opens the Audit Trail Viewer window, which lists existing audit records and jobs for the selected record.
Schedule	Opens the Scheduling Action Group window, where you define a schedule for the selected compliance policy group. Click the Schedule tab and define start/stop time, recurrence, and whether to enable the schedule.
Delete	Removes the selected compliance policy groups.
Share with User	Opens the Share with User window where you select the colleague you want to share this asset with and then type your message.

Compliance Policies/Proscan

Use the Compliance Policies/Proscan portlet to configure compliance requirements. Limit the visible policies using the filtering in the expanded view.

This portlet is intended for users who are interested in configuring and maintaining compliance policies or policy groups.

Access this portlet from the Configuration Management > Compliance navigation bar. This portlet has both a summary view and an expanded view. Each view could display different columns and has the same pop-up menu options available.



Columns

Other than the general navigation and configuration options, the Compliance Policies/Proscan portlets (summary and expanded views) include the following columns. The columns displayed by default are noted.

You can view the value for most of the hidden columns by clicking the Settings tool, selecting the columns tab, clicking Show for the appropriate column, and then applying the change.

Column	Description
Name	The user-defined name for the policy or policy group. This field displays on the summary and expanded views by default.
Targets	The number of devices to scan. This field displays on the summary and expanded views by default.
Overall Compliance	The overall policy compliance using the following values and flags: • **All Compliant**—Icon: Green. indicates that all selected equipment is in compliance with the policy. • **None Compliant**—Icon: Red. indicates that none of the selected equipment is in compliance with the policy. • **None Determined**—Icon: blank. indicates that none of the equipment was tested for compliance. • **Partial Compliance**—Icon: Yellow. indicates that not all equipment complies with the policy but all equipment was tested. • **Compliance Varies**—Icon: Yellow indicates that not all equipment was tested for compliance. The tested equipment might be compliant or not compliant. This field displays on the summary and expanded views by default.
Monitored	An indicator that shows whether the policy is monitored (checkmark) or not (X). See ProScan on page 211 in Performance Monitoring for details. This field displays on the summary and expanded views by default.
Scheduled	An indicator that the policy's execution is scheduled (Yes) or not (No) and whether the schedule has occurred. This field displays on the summary and expanded views by default. **Note:** You can execute a policy manually from the Managed Resources portlet by right-clicking the targeted device, selecting Change Management, and then selecting one of the following options: • **Execute ProScan** to execute policies that target the device. • **Execute Proscan Policy** to execute a ProScan policy that is not already associated with the device or group. A selection screen appears where you can select a policy and either execute or schedule it.
Description	A detailed description of the policy/policy group. This field displays on the expanded view by default.
Enabled	An indicator that shows whether the policy is enabled (checkmark) or not (X). This field displays on the expanded view by default.
Proscan Type	An indicator that the policy is a single policy or a group policy. This field displays on the expanded view by default.
Input Source	The inputs source, such as Not Applicable, Current Label, and so on. This field displays on the expanded view by default.

Column	Description
Next Execution Date	The frequency in which to execute the scheduled action, such as each weekday, every three months, only at startup, only once, and so on. This field displays on the expanded view by default.
Icon	A graphical representation of the selected policy/rule.
Widgets	Additional information about the selected alarm, such as: • Reference Tree shows the connection between the alarm and its resource. • Compliance Policy Summary catalogs the compliance policy's history and lists the equipment scanned and a indicator that the run discovered equipment in (checkmark) or out (X) of compliance. • Compliance Policy Chart The Widgets field is available **only** from the expanded view.
Adaptive CLI	The Adaptive CLI script.
Config File Label	The configuration file label, such as Current.
Configured Date	The configuration date and time.

Pop-Up Menu

The Compliance Policies/Proscan pop-up menu provides access to the following options. Right-click a row to access these options.

Menu Option	Description
New	Select either a new policy or group. Creating a new policy opens the ProScan Policy Editor, through which you can define one. See Creating or Modifying a ProScan Policy on page 325 for more information about the Editor. See Creating or Modifying ProScan Policy Groups on page 339 for the group editor. Provides access to the following options to create policies/policy groups: • Group opens the Creating New Compliance Policy Group window, where you define general properties, grouped policies, and grouped targets. See Creating or Modifying ProScan Policy Groups for editor details. • Policy opens the Creating New Compliance Policy, where you define a policy's general properties, targets, and compliance criteria.
Edit	Opens the selected policy or group for modification. See Creating or Modifying a ProScan Policy on page 325 for more information. See Creating or Modifying ProScan Policy Groups on page 339 for the group editor.
Execute Compliance	Initiates a compliance check for the selected policy. The Job Status window opens displaying each check as it occurs and its outcome as well as a Success/Failed when complete. This option is available only for compliance alarms.
Refresh Targets	Queries to check targets, particularly those in dynamic groups, are up-to-date. Best practice is to Refresh ProScan Targets before running a scan particularly if your network has changed since the last scan. You can also schedule this. See Schedule on page 671.
Modify Targets	Lets you modify and/or select target equipment for the policy.
Schedule	Configures a policy to run on a schedule.
Audit	Opens an Audit Viewer with the results of a selected policy's runs. This is one way to see the historical results of the ProScan policy runs. Another is to consult the Compliance Policy Summary widget in the Compliance Schedules.
Delete	Removes the selected compliance policy/group. **Caution:** This can impact anything that refers to what you are deleting.

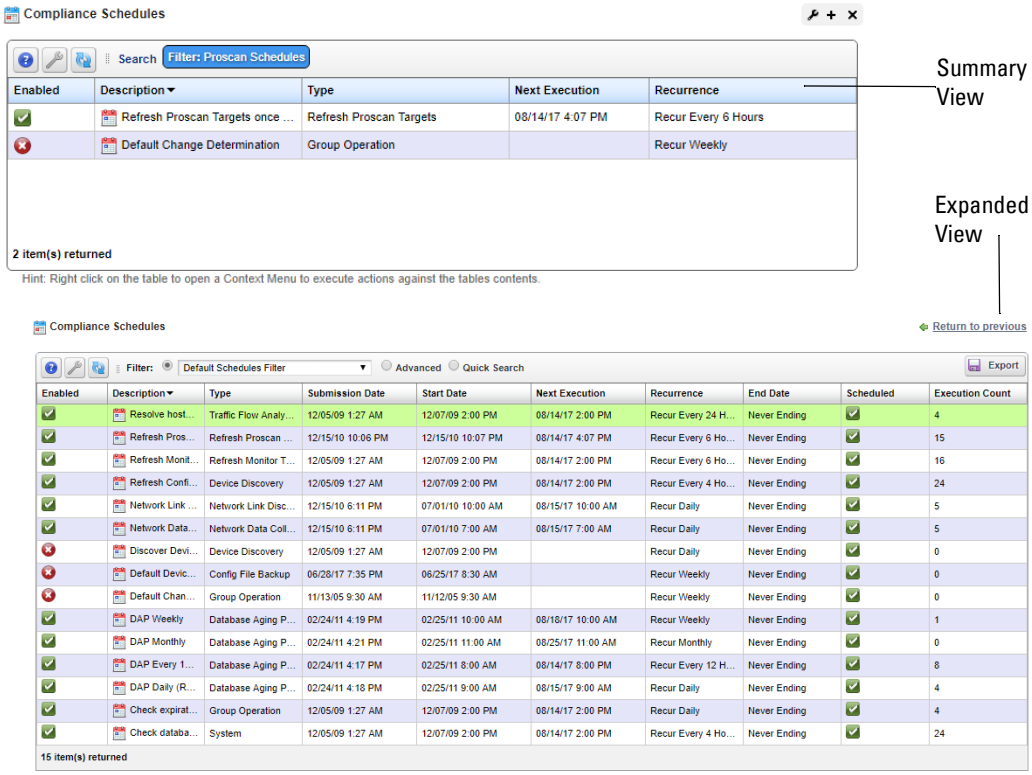
Menu Option	Description
Import/Export	Provides the following actions when available for the selected image: • Import retrieves a file containing XML compliance descriptions. Some imports can come from a URL. • Export Selection exports the selected description to an XML file. • Export All exports all descriptions to an XML file. Click Download Export File to specify where to save the file. The Import/Export option is useful as a backup or to share descriptors with other projects. You must import data into the correct portlet. For example, you cannot import event data into the Actions portlet. If one type of data depends on another, you must import the other data before importing the data that depends on it.
Share with User	Opens the Share with User window where you select the colleague you want to share this asset with and then type your message.

Compliance Schedules

Use the Compliance Schedules to view and modify ProScan-specific schedules. You can use Schedules to initiate the Change Determination process. See Change Determination Process on page 344. Change Determination is disabled by default.

This portlet is intended for users who are interested in viewing and modifying ProScan-specific schedules.

Access this portlet by selecting Configuration Management > Compliance from the navigation bar. This portlet has both a summary view and an expanded view. Each view could display different columns and has the same pop-up menu options available.



Columns

Other than the general navigation and configuration options, the Compliance Schedule portlets (summary and expanded views) include the following columns. The columns displayed by default are noted.

You can view the value for most of the hidden columns by clicking the Settings tool, selecting the columns tab, clicking Show for the appropriate column, and then applying the change.

Column	Description
Enabled	An indicator that shows whether the schedule is enabled (checkmark) or not (X). This field displays on the summary and expanded views by default.
Description	A detailed description of the scheduled action, Network Data Collection, Default Device Config Backup, and so on. This field displays on the summary and expanded views by default.
Type	The type of action scheduled, such as Device Discovery, Config File Backup, Database Aging Policy, System, and so on. This field displays on the summary and expanded views by default.
Next Execution	The next date and time that the schedule will execute. This field displays on the summary and expanded views by default.

Column	Description
Recurrence	The frequency in which to execute the scheduled action, such as each weekday, every three months, only at startup, only once, and so on. This field displays on the summary and expanded views by default.
Submission Date	The date and time that this schedule was submitted. This field displays on the expanded view by default.
Start Date	The date and time to start the scheduled action execution. This field displays on the expanded view by default.
End Date	The date and time to end the scheduled action execution or the number of occurrences before ending this scheduled action. This field displays on the expanded view by default.
Scheduled	An indicator that shows whether definition is scheduled (checkmark) or not (X). This field displays on the expanded view by default.
Execution Count	The number of times this scheduled action executed. Useful if you specified and end date based on the number of occurrences. This field displays on the expanded view by default.
Domain ID	The identifier for the resource domain.
Run Status	Indicated the schedules current state, such as waiting.

Pop-Up Menu

The Compliance Schedules pop-up menu provides access to the following options. Right-click a row to access these options.

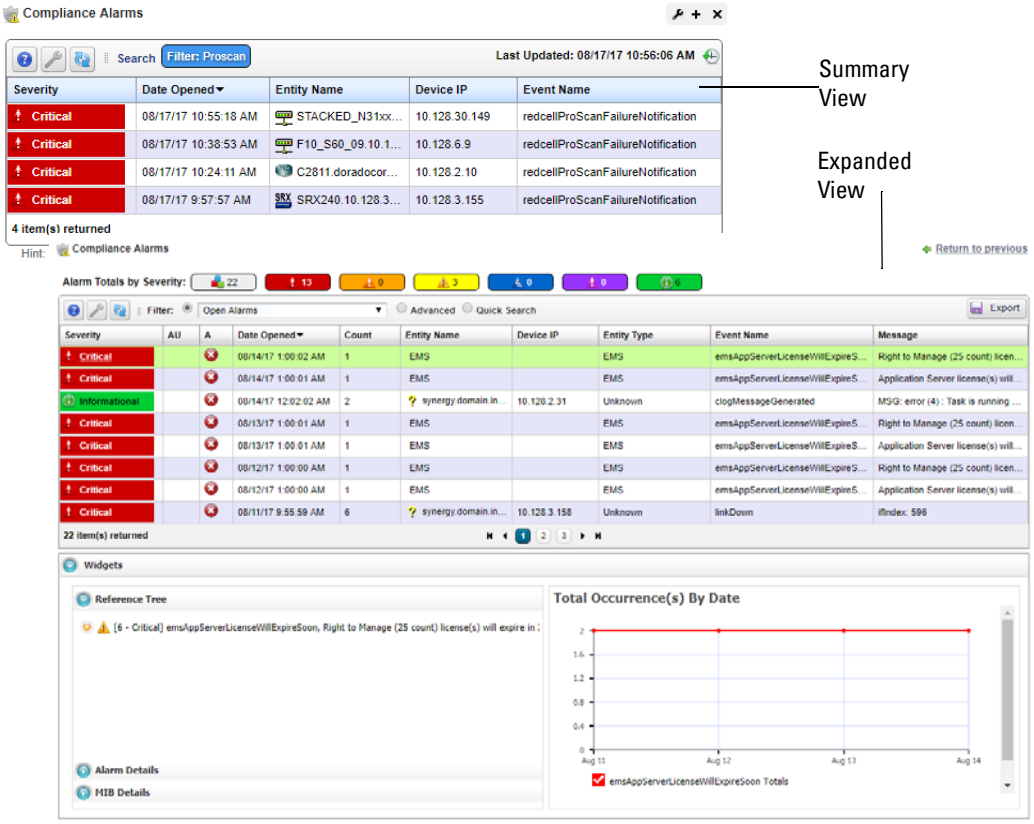
Menu Option	Description
New	Opens the New Schedule window, where you define a schedule for the following option selected: • Action (see Scheduling Actions on page 307 for the details) • Alarm Suppression (See Managed Resources on page 454 for details) • Config File Backup • Config File Restore • Database Aging Policy (Implementing DAP on page 38 for more about DAP) • OS Image Deploy The subsequent window's fields and options depend on the action selected.
Edit	Opens the Editing Schedule (*proscanTarget*), where you modify the schedule settings.
Delete	Removes the selected schedule. A successful/unsuccessful confirmation message is displayed.
Disable Schedule	Deactivates a currently enabled schedule. This option displays if the selected schedule is currently enabled. You can also disable a schedule by right-clicking it and then selecting the deselecting the Enable Schedule option from the Editing Schedule window.
Enable Schedule	Activates a currently disabled schedule. This option displays if the selected schedule is currently disabled. You can also enable a schedule by right-clicking it and then selecting the Enable Schedule option from the Editing Schedule window.
Execute	Runs the actions for the selected schedule. The audit viewer displays execution progress for activity-based or discovery-profile-base schedules. For all other types of scheduled actions, a message is displayed stating that the item was sent to the application server for immediate execution. Monitor it progress from the Audit Trail portlet (see Audit Trail Portlet on page 630 for more details).
Share with User	Opens the Share with User window where you select the colleague you want to share this asset with and then type your message.

Compliance Alarms

Use the Compliance Alarms portlet to manage ProScan-related alarms. This portlet filters all other non ProScan-related alarms.

This portlet is intended for users who are interested in managing ProScan-related alarms.

Access this portlet by selecting Configuration Management > Compliance from the navigation bar. This portlet has both a summary view and an expanded view. Each view could display different columns and has the same pop-up menu options available.



Columns

Other than the general navigation and configuration options, the Compliance Alarms (summary and expanded views) include the following columns. The columns displayed by default are noted.

You can view the value for most of the hidden columns by clicking the Settings tool, selecting the columns tab, clicking Show for the appropriate column, and then applying the change.

Column	Description
Severity	The alarm severity indicated by the color and text. The severity only has meaning for alarms and security alarms. Informational alarms have a severity level of Indeterminate. Closed alarms show without color. This field displays on the summary and expanded views by default.
Date Opened	The date the alarm was created. This field displays on the summary and expanded views by default.

Column	Description
Entity Name	The entity emitting this alarm. This field displays on the summary and expanded views by default.
Device IP	The equipment IP address where the alarm appeared. This field displays on the summary and expanded views by default.
Event Name	The event associated with the alarm. This field displays on the summary and expanded views by default.
Assigned User (AU)	The user currently assigned to this alarm. You can filters your assigned alarms using the Advanced filter option and selecting Assigned by User, contains, and entering your user ID. This field displays on the expanded view by default.
Acknowledged (A)	An indicator whether the alarm is acknowledged (checkmark) or not (X).
Count	The number of instances for this alarm. Multiples of the same alarm show as a single row but this value increments as more instances occur. This field displays on the expanded view by default.
Entity Type	The type of monitored entity. This field displays on the expanded view by default.
Message	The message associated with the alarm. This field displays on the expanded view by default.
Widgets	Additional information about the selected alarm, such as: • Reference Tree shows the connection between the alarm and its resource. • Alarm Details shows the severity, message, date opened, and so on. • MIB Details shows notification OID and MIB text. • Total Occurrences by Date shows a graph of the total occurrences by date. The Widgets field is available **only** from the expanded view.
Alarm State	The alarm's open or closed state.
Date Cleared	The date and time the alarm was closed.
Updated Date/ Time	The time stamp for when the alarm was updated.
Notification OID	The identifier for the notification displayed as an alarm.
Equipment	The entity emitting the alarm.
Date Assigned	The date and time that the alarm was assigned.
Assigned By	The user ID for the person that assigned this alert.
Ack Time	The time that the alarm was acknowledged.
Cleared By	The user ID for the person that cleared the alarm.
MIB Text	The alarm's MIB text.
Ack By	The user ID for the person that cleared the alarm.
Correlated By	The date and time when the alarm correlation to a parent alarm (caused by or blocked by).
Correlated Time	The role the alarm plays in any correlation, such as top-level alarm, caused by parent, blocked by parent.
Correlation State	The domain emitting the alarm.
Domain ID	The identifier for the resource domain.
Entity Description	The alarmed entity's description.
Has Children	An indicator that shows whether the alarm has children (checkmark) or not (X).

Column	Description
Highest Severity	The highest severity assigned to the selected alarm.
Location	The alarm's location.
Notes	A text field for information about the resource.
Original Severity	The original severity specified for the selected alarm.
Parent Alarm	The name of the parent alarm.
Region	The alarm's region.
Resource Propagation	The propagation for this alarm, if any.
Service Affecting	Indicates whether the alarm is on equipment in a provisioned service (checkmark) or not (X). A service affecting alarm propagate to show as a component of service- and customer-related alarms. Service-Affecting alarms are of indeterminate or greater severity.
Suppressed	An indicator whether the alarm is suppressed (checkmark) or not (X).
Suppression Date	The date and time of the alarm's suppression, if applicable.
Suppression End	The alarm's suppression termination.
Suppressor	The alarm that suppresses the selected alarm.

Pop-Up Menu

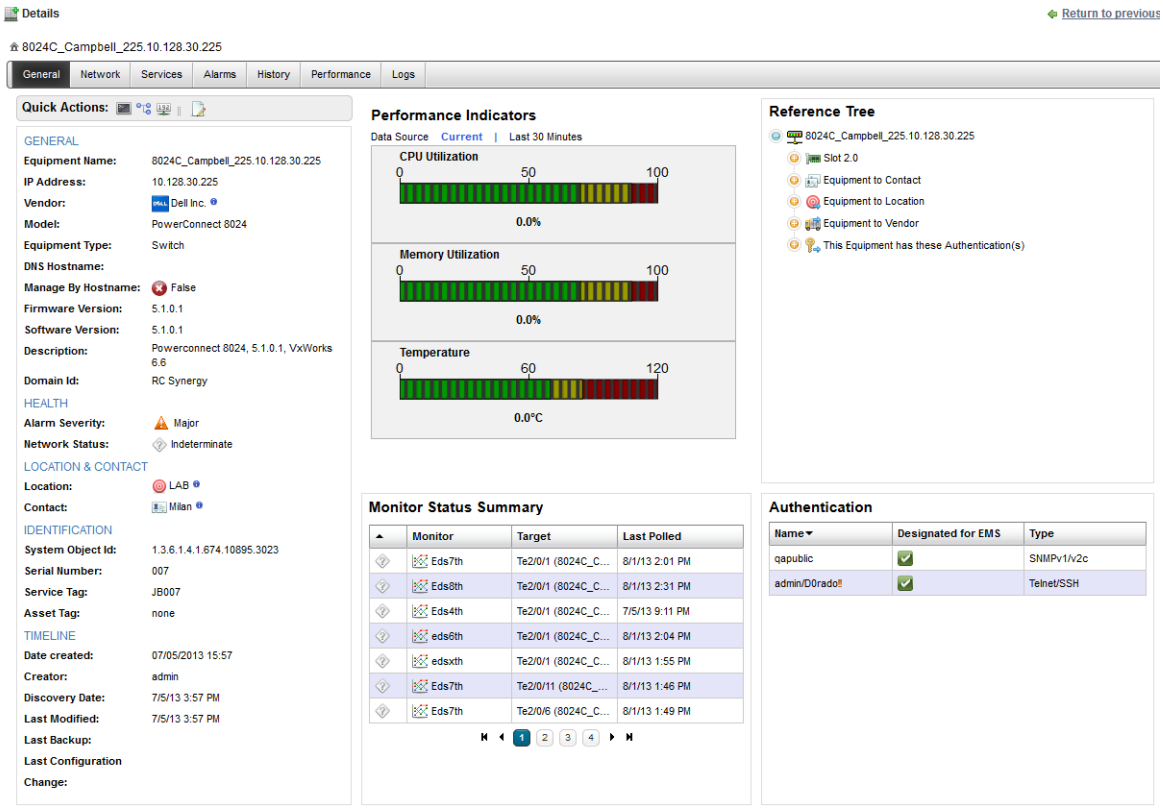
The Compliance Alarms pop-up menu provides access to the following options. Right-click a row to access these options.

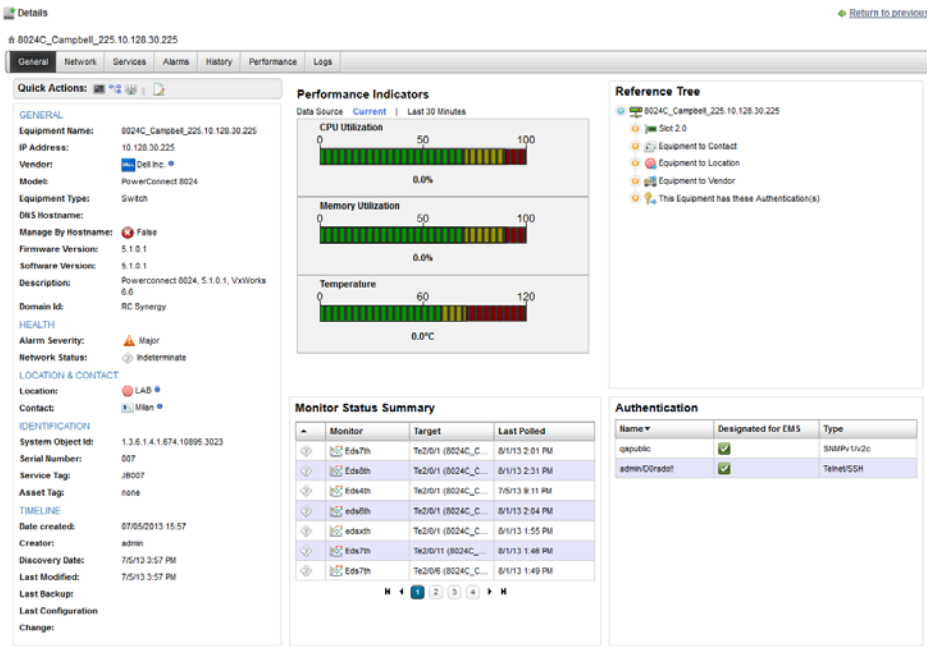
Menu Option	Description
Edit	Opens the Edit Alarm window or Editing Event Definition window, where you modify the alarm or event definition, respectively.
Details (Click+Shift)	Displays either equipment or alarm details, such as general information, MIB text, reference tree, advisory text, event processing rules, correlations, performance, and so on. The details displayed vary depending on the option selected (Alarm Details/ Equipment Details).
Visualize	Displays a topology map that includes the selected alarms. See Using Visualization Tools for more about these maps.
Acknowledge Alarm	Acknowledges the selected alarms. The current date and time appear in the Ack Time field. The checkmark appears in the expanded portlet for acknowledged alarms. This option is available when the selected alarms **are not** acknowledged.
Unacknowledge Alarm	Unacknowledges previously acknowledged alarms, and clears the entries in the Ack By and Ack Time fields. When an alarm is not acknowledged, the red icon appears in the expanded portlet. This option is available when the selected alarms **are** acknowledged.
Assign User	Assigns this alarm to one of the users displayed in the sub-menu by selecting that user. An icon also appears in the expanded portlet indicating the alarm is assigned to someone.
Clear Alarm	Removes the alarm from the default alarm view and marks it as a candidate for the database archiving process (DAP). Clearing an alarm is an indication to the system that the alarm was resolved/addressed. If your system has propagation policies enabled, clearing recalculates dependent alarms.

Menu Option	Description
Clear Group of Alarms	Removes a group of alarms from the default alarm view and marks them as candidates for DAP. This option is useful when you have many unimportant alarms that you want to clear at the same time instead of individually. For example, perhaps you want to clear all alarms that are informational and are more than a week old. Before selecting this menu item, create a filter for the group of alarms that you want to clear. When you select Clear Group of Alarms, a list of defined filters appears. Select the appropriate filter and then click Execute. All open alarms that meet the filter criteria are cleared. **Caution:** The Clear Group of Alarms action is irreversible.
Direct Access	Open an SNMP Mib Browser to the alarmed device, a CLI Terminal (Telnet window) to the alarmed device, or ICMP Ping the device alarmed. Only those available appear in the subsequent menu.
Email Alarm	Opens the Email Alarm window, where you specify a subject and e-mail address to which you want to mail the alarm's content, and then click Send Email. Click Cancel to end this operation without sending e-mail. SMTP setup is required to e-mail an alarm. See SMTP Configuration on page 626 for instructions about setting up e-mail from OpenManage Network Manager.
Show Performance	Shows performance data for the selected interfaces in the Performance Dashboard window. Click the edit tool to modify the dashboard view properties, entities, or attributes. See Dashboard Editor on page 227 for more about the editor and its options.
Aging Policy	This lets you select a policy that determines how long this alarm remains in the database. See Implementing DAP on page 38 for information about configuring such policies.
Edit Custom Attributes	Opens the Custom Attribute Editor where you define field characteristics, such as whether it is enabled, the label name, and the tooltip.
View as PDF	Creates an Acrobat PDF document containing this alarm's contents displayed in the summary portlet.
Share with User	Opens the Share with User window where you select the colleague you want to share this asset with and then type your message.

Equipment Details

This screen displays the details for a selected resource. You can see it by selecting *Details* in the right-click menu for the Managed Resources portlet. You can also install an Equipment Details portlet on a page and use the Container View portlet to select individual devices that appear in it. In that case, you must select an individual device before it displays data.





Details screens are available for a variety of things besides equipment, too. Here are some highlights of the Equipment Details screen (and others):

The *Quick Actions* panel in the General tab also displays icons that activate direct access or the resource editor.



Direct access includes Terminal, MIB Browser, Ping (ICMP) or HTTP / HTTPS).

Click the tab name to see the following:

General–In addition to Quick Action icons, this displays details about the selected equipment, including its Domain ID. This screen also includes performance indicators to report on the device's CPU, memory and disk utilization (flash memory) both currently and for the last 30 minutes (click the links above the panel), a Monitor Status Summary, and Reference Tree, and a list of the Authentications connected to the device. If disk utilization is less than one percent, an indication that the device is still active may appear in that graph.

Permissions control the visibility of some attributes. Information like IOS/Firmware/Software versions appears to users only if they have READ permission for these attributes. To configure attributes as not viewable—one example: management IP address—you must define the attribute set and add it to `owareapps\installprops\lib\installed.properties` as in the following example:

```
restricted.attribute.names.set1=RedCell.Config.EquipmentManager_IPAddress
```

For each restricted attribute set, you can define multiple attributes with comma delimited DSI names.

After defining such attributes, in the permission manager, uncheck the READ permission on roles that you do not wish to have access to `Restricted Attribute Access 1`. You can conceal up to five such attributes. Attribute names are similar to the Using Email Action

Variables on page 100, at least when fully qualified with the prefix `Redcell.Config.EquipmentManager`. Contact technical support for identifiers not listed there.

Network–This screen lists the Ports and Interfaces for the selected device (some devices have one, but not the other), VLANs and links associated with the device.

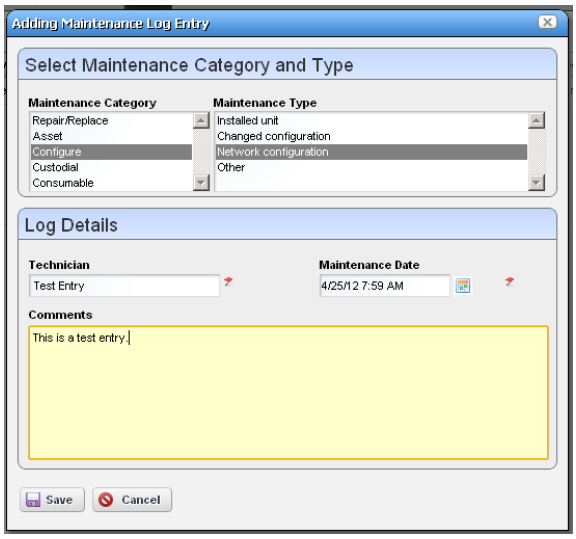
Alarms–Displays the alarms and events associated with the selected device.

History–Includes audit trails connected to the device, and any backed up configurations. Right-click to view or otherwise act on these.

Performance–This screen contains two links at its top. One displays a performance dashboard (template) related to the selected device. See Show Performance Templates on page 232 for how to configure these. The other displays any configured *Top Talkers* for the device. See Top N [Assets] on page 220.

You can also configure the interval displayed by clicking the clock icon at the top of this screen.

Logs – Displays maintenance logs connected to the device to users with permissions to see this tab. Right-click to create or edit these.



Notice that you can right-click listed interfaces, configuration files, and so on to perform more actions, or to see additional Detail screens.

You can also right-click and then select *Details* to view more information about some subcomponents like Interfaces and Ports. The Details portlet includes a *Reference Tree* (similar to the Widgit). You can even right-click nodes in that reference tree to drill down to additional details.



NOTICE

Notice the breadcrumb trail at the top of the Equipment Detail panel tracks the levels through which you drill down. You can click a level that appears in this trail to return to a previous screen. If you click *Return to previous* in the upper right corner of the screen, you will return to the original screen from which you selected the basic equipment.

Also: Some fields may appear truncated onscreen, but you can hover the cursor over the truncated field so the text appears as a tooltip or drill down to see the detail.

Some devices populate the ports panel, but not the interfaces panel, which is empty for such devices. Interfaces may appear for Dell EMC Networking FTOS, Cisco or Juniper devices. You may also discover such devices as type: Unknown (see Base Driver on page 66). Force 10 devices interfaces details can display Port Channels (LAGs), VLANs (SVIs) and Loopbacks.

If the Ports portlet is on the same page as the Managed Resources portlet, selecting a device in Managed Resources makes its ports appear in the Ports portlet. The display can also get out of sync, but clicking the browser's *Refresh* restores the correspondence between a selected device and the ports displayed. To resync a port, resync the device that contains it.

Field Definitions

The meanings of most fields that appear in details screens are self-evident. Here is a little more information about some of them:

Operational State—One of following possible values describing the availability of the resource.

Disabled—Inoperable because of a fault, or resources are unavailable.

Enabled—Operable and available for use.

Active—Device is operable and currently in use with operating capacity available to support further services.

Busy—Operable and currently in use with no operating capacity to spare.

Administrative State—One of the following values:

Locked—Device use is prohibited.

Shutting Down—Only existing users can use the device.

Unlocked—Normal use of device is permitted.

Network Status—The status of the resource in the network. For example: *Responding* means this application can, via some network protocol, get the device to respond. *Not Responding* means the device does not respond to the protocol. *Indeterminate* means the monitoring software has not tried to reach the device or there was some other error which prevented us from determining one of the other two statuses.

The appearance of *Network Status* depends on the default ICMP monitor (see Resource Monitors on page 169. If you exclude this equipment from the monitor or disable it (for example, for performance reasons) then a status may appear, but it is not meaningful.

You can now use monitors other than ICMP to determine this status. See Monitor Network Availability— Alternative Method on page 173.

NOTE:

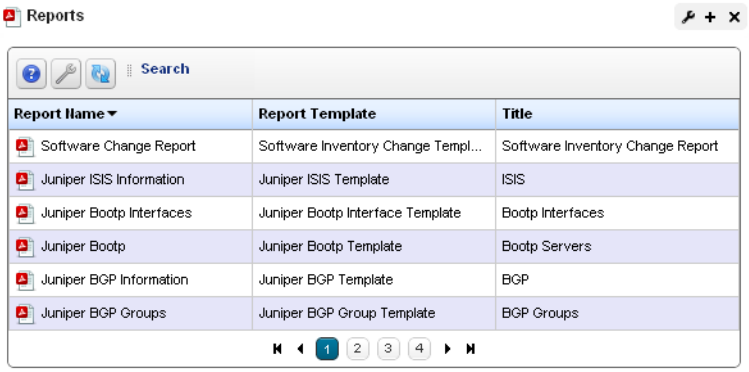
The Alarms Details panel now lets you correlate parent/child alarm pairs.

Reports Page

Reports Portlet

Reports Portlet

This portlet's summary screen lists the available reports that you can run with OpenManage Network Manager.



The report *Icon*, *Name*, *Template*, and *Subtitle* appear in the columns in this summary screen. Generally speaking, the report selects the target equipment, and the template configures the layout and attributes reported. If the Interface details panel is empty, then the Interface reports will have no contents. Some devices have ports, but no interfaces. Use the Ports report for such devices.

OpenManage Network Manager generates reports with only the first 5,000 records by default. Larger reports warn that they have reached the maximum, and have only those first 5,000 records.

You can change the maximum with the property
`com.dorado.redcell.reports.max.report.query.size=5000`

in rpt.properties file in /owareapps/reports/lib/.

Larger numbers have an impact on the performance of the report and database.

NOTE:

You must have Adobe's Acrobat reader installed to view reports.

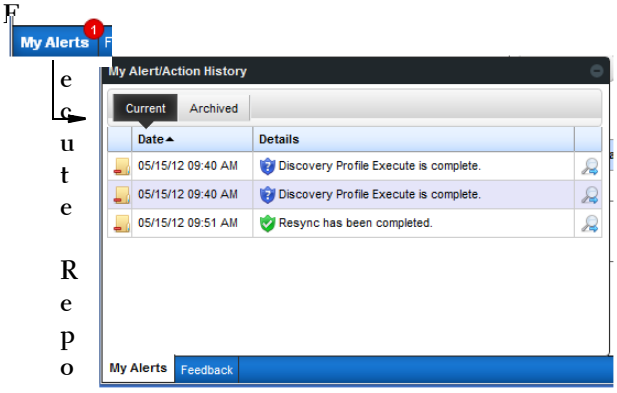
Right-click a selected report to do the following:

New / Edit / Copy —This opens the Report Editor, described below, to configure a new report, edit or copy an existing, selected report. *Copy* automatically renames the selected report.

New Group—Creates a collection of reports. See Printing Groups of Reports on page 133 for details about how to configure these.

Schedule—Opens a scheduler screen to automate report creation.

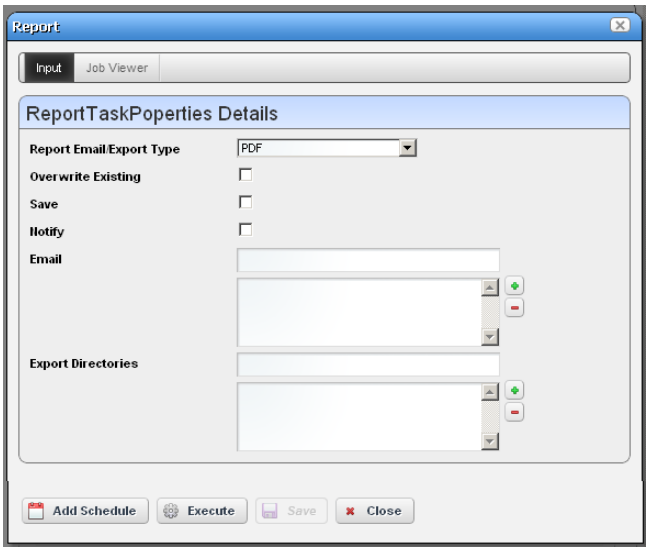
F



e c u t e R e p o r t — When you execute a report, a numbered message notification appears, and a link to the report appears in the *Messages* panel to notify you the report is ready for viewing. Click the magnifying glass to the right of the notification to view either the audit trail or the report.

Lengthy Reports may take a some time to appear onscreen without much indication that they are in process. This is an artifact of the Acrobat plug-in, and outside the scope of OpenManage Network Manager to influence. Acrobat also produces an error if a report has too much data to display meaningfully.

Execute Report (Advanced)—Also lets you schedule configure a few other things with reports.



When you *View or Execute Report (Advanced)*, by right clicking either a listed report or a historical instance of that report, a configuration screen appears that lets you select several parameters.

These include the following:

Report Email / Export Type—Select the export file type from the pick list. Options can include *CSV*, *HTML*, and *PDF*.

NOTICE

Programs other than OpenManage Network Manager let you manipulate mail outside the scope of OpenManage Network Manager. For example IFTTT (If This Then That) could save mail attachments like reports to Dropbox accounts. **Also:** Open CSV output in a spreadsheet for additional formatting options.

Overwrite Existing—Check to activate overwriting any existing report.

Save—Check to activate saving the report to the database.

Notify—Check to activate emitting a notification event.

Email Address—Enter an e-mail destination for the generated report, and click the plus (+) to list it. You can enter several such e-mails.

Export Directory—Enter directory destinations for saved reports as you would e-mail destinations.x

Click *Add Schedule* to schedule the report for future or repeated execution, *Execute* to run the report immediately, or *Save* to preserve this report's configuration. The *Job Viewer* tab displays the report's progress if you click *Execute*.

CAUTION:

Reports can be large. Typically the limitations on e-mail within your system are what limit the size of deliverable reports. Best practice is to use filters and a limited number of targets to make reports succinct rather than comprehensive.

Aging Policy—If you automate report generation, you may also want to configure a Database Aging Policy to insure the volume of reports does not overwhelm your storage capacity. See Implementing DAP on page 38 for more about doing that.

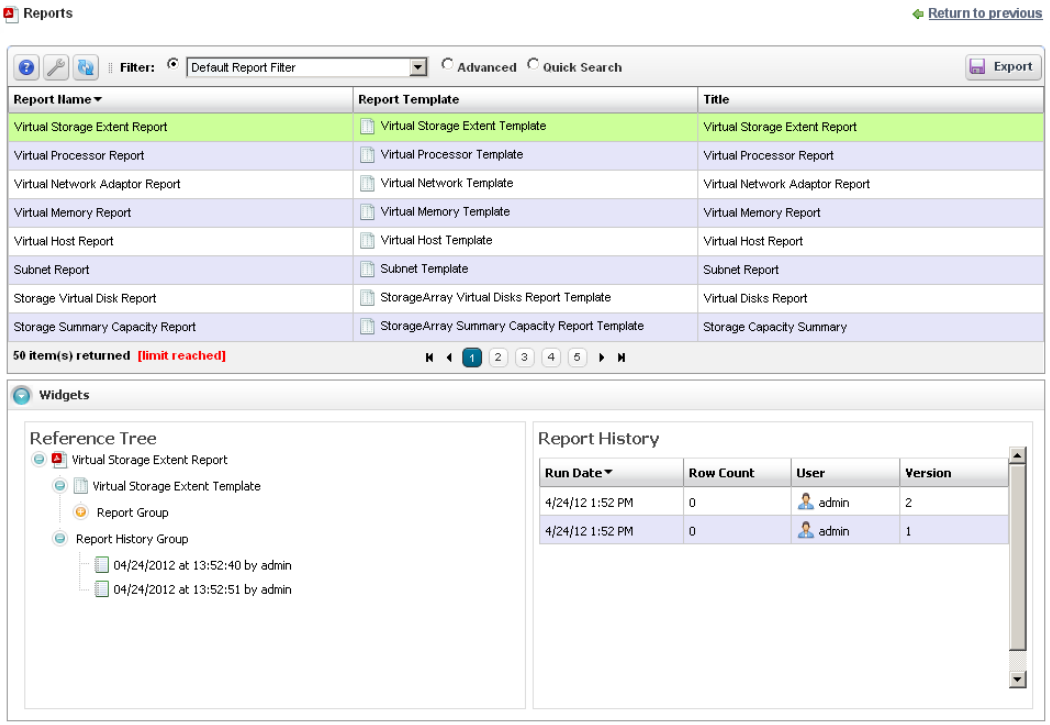
Delete—Removes the selected report from the list display

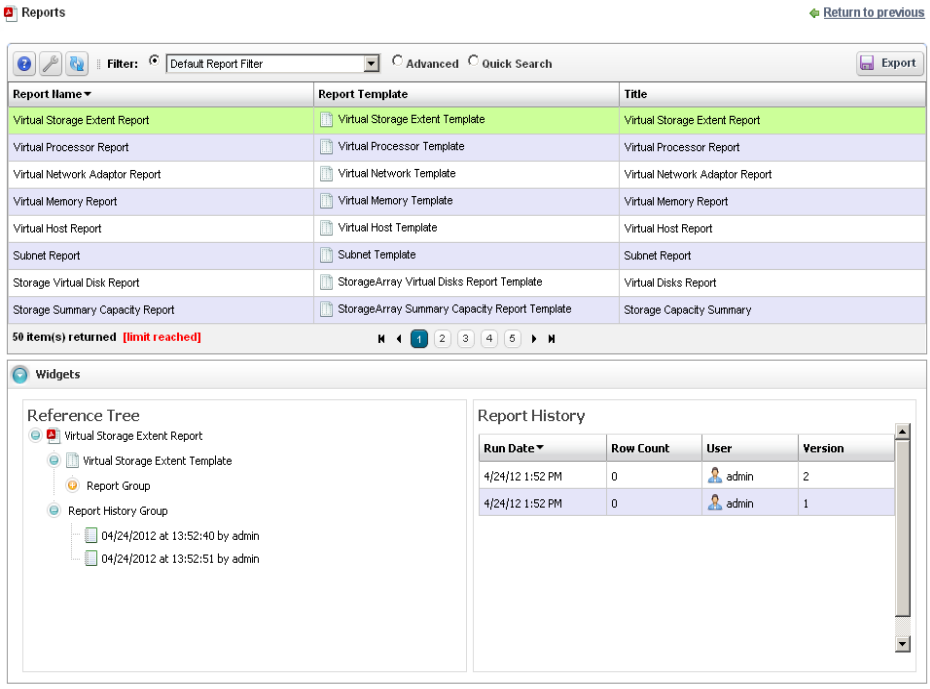
Delete History—Removes the selected report's history.

To change reports' appearance and contents, you must configure their Report Templates Portlet. Also, see Branding Reports on page 132 for instructions about changing the default report logo.

Expanded Reports Portlet

Clicking the plus (+) icon displays the expanded portlet. the expanded portlet adds *Add / Remove Column* to the menu options available in the summary screen.





Available columns are like those described in the summary screen section previously. The *Reference Tree* snap panel displays the selected report's connection to devices, historical reports and any report template. Right-click to view the reports in the Historical Reports node.

Reports Snap Panels

The Snap Panels for reports display a Reference Tree of connections between the selected report and target equipment, and between the report and any Report Template.

The *Report History* Snap Panel displays the selected report's *Run Date*, *Row Count* and the *User* who ran the report. Right-click a row in this panel, and you can *Delete*, *Print* (the report history) or *Export* (the report history), *View* (the report) or *View (Advanced)*. If you *View* the report, a message with a link to the report appears in the bottom left of the screen.

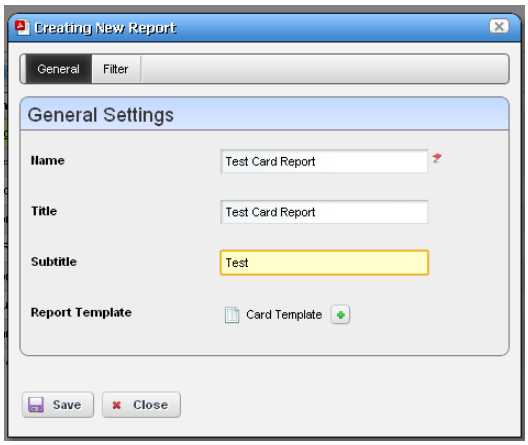
Report Editor

This editor configures reports, and their targets. It has the following screens and fields:

- General
- Filter

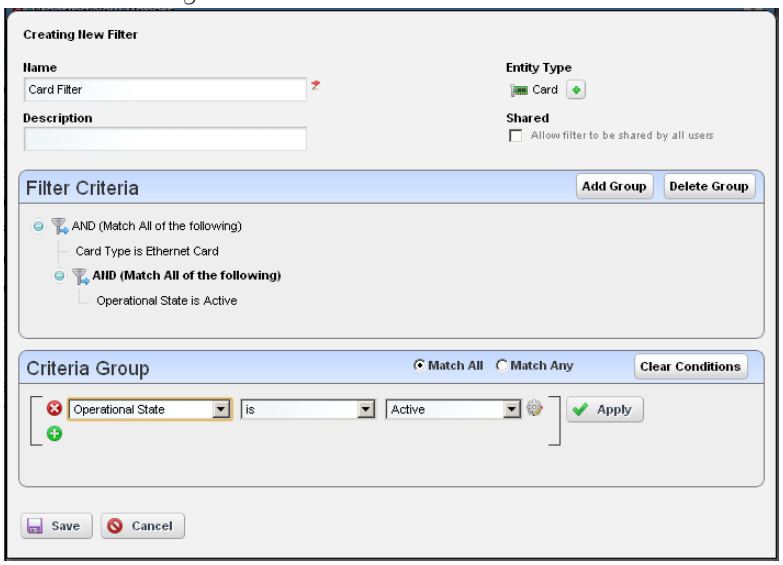
General

This screen configures the *Name*, *Title* (displayed text in the report), *Subtitle*, and lets you select the *Report Template* for the report (see Report Templates Portlet on page 618 for more about them)



Filter

This screen configures a filter to retrieve devices that are the source of the report.



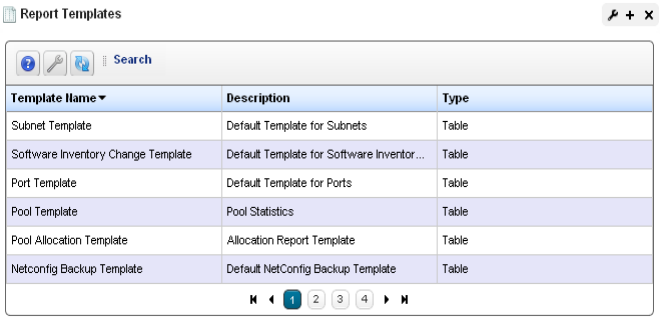
Click *Add Filter* in the filter panel to select an existing filter, create a new filter, or copy an existing filter. When you create a new filter, you must enter a *Name* and optionally a *Description* for it, select an *Entity Type* with the green plus (+), and elect whether this filter is available to other users *(Shared)*. See Defining Advanced Filters on page 86 for instructions about configuring the filter itself in the lower portion of this screen.

Once you have configured or selected a filter, the *Filter* panel displays its characteristics in tree form. Click *Edit* to re-open the editor, or *Del* to remove the filter. Filters appear only fro the entity type of your report template.



Report Templates Portlet

Report Templates are the basis of reports. This portlet displays the *Template Name*, *Description*,



Inventory Entity, and *Type* in columns.

Right-clicking in this portlet lets you create a *New* template, *Edit* a selected template (see Report Template Editors for information about subsequent screens), view *Details* or *Delete* a selected template. You can also *Import* / *Export* report templates to files.

The expanded Report Templates portlet also includes a Reference Tree snap panel displaying a tree for selected templates connecting them to Report Groups and specific reports.

NOTICE

You can create reports related to users and their groups. Create a new report and select *Permission* as the Source of attributes in Report Template editor to begin.

Report Template Editors

OpenManage Network Manager has several report template editors. Creating a *New* template, can make *Comparison*, *Table* and *Trend* templates.

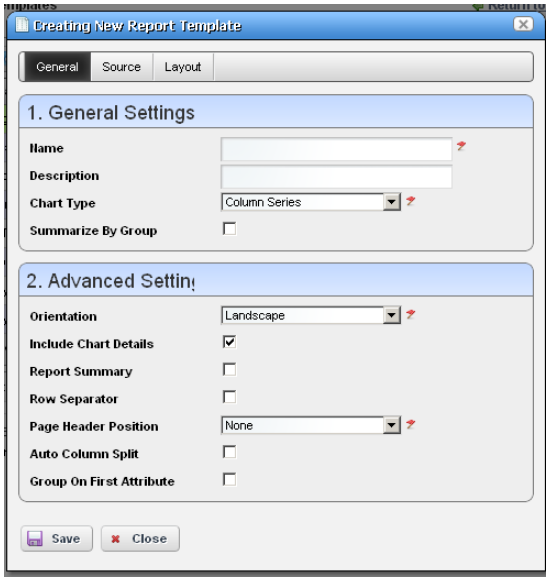


Table reports simply report the configured data in tabular form as you have configured the columns. Comparison reports display selected attributes comparing reporting devices, for example a summary graph then a list of devices' ICMP monitor RTT in the following pages.

A Trend Report displays a data graph with data reported over a polled period.

You can now select more than one attribute for trend reports. Chart generation depends on the number of attributes selected and the number of targets:

- 1 target, n attributes produces 1 chart with all attributes (line series graph only)
- n targets, 1 attribute produces 1 chart with all the targets
- x targets, n attributes produces n charts with x targets on each

This editor has General, Source, and Layout tabs.

You can edit any but pre-existing templates, whether they have reports attached to them or not. Consider this example:

Template T has three columns; A, B and C. Someone creates a report R against Template T, executes the report, saves the data as a historical report H1. Two weeks later, someone modifies the Template T, removing column C, adding column D.

When executing report R against the revised Template T', the report now shows columns A, B and D. User saves the report as historical report H2. Here, H1 only has data for columns A, B and C. H2 has data for columns A, B and D.

If you view H1 you see Template T' is in use and this template creates a report with columns A, B and D. Unfortunately, H1 only has data for columns A, B and C, so the report created has data for columns A and B only. Column D is empty. When viewing H2 you can see Template T' is in use and can create a report with columns A, B and D. H2 has data for columns A, B and D, so all data appears.

General

The following are fields that appear on these screens. Not all screens have all fields.

General Settings

Name—An identifier for the template.

Description—An optional description of the template.

Chart Type—Select from the available alternatives (*column*, *line*). This is only available for trend and comparison templates.

Summarize by Group—Group similar results together. This is only available for trend and comparison templates

Advanced Settings

Orientation—Select from *Portrait* and *Landscape*

Include Chart Details—Includes a table with the data after the graph. This is only available for trend and comparison templates

Report Summary—Enables the report summary, which places the total count of records at the end of the report.

Row Separator—Displays a separator between rows within the report.

Page Header Position—Select *none*, *top*, *bottom* or *both*.

Auto Column Split—Enable automatic column splitting. This automatically aligns the columns equally on the report providing the column widths that are most proportional.

Group on First Attribute—Creates a report that groups rows based on the first reported attribute. This creates groups of items in the report whenever the left most column's value changes.

For example, with disabled, a report looks like this:

Device Name	Gig/e Port Name	Health Status
M5	ge/0/0/1	Up
M5	ge/0/0/2	Down
M5	ge/0/0/3	Up
M5	ge/0/0/4	Unknown
M18	ge/0/1/1	Up
M18	ge/0/1/2	Starting
M18	ge/0/1/3	Up
M18	ge/0/1/4	Down

The same report looks like this with *Group on First Attribute* enabled:

Device Name	Gig/e Port Name	Health Status
M5		
ge/0/0/1	Up	
ge/0/0/2	Down	
ge/0/0/3	Up	
ge/0/0/4	Unknown	
M18		
ge/0/1/1	Up	
ge/0/1/2	Starting	
ge/0/1/3	Up	
ge/0/1/4	Down	

Alternative ways of Grouping Attributes in Reports—The following are ways to turn on grouping in a report template.

- *Select Group on First Attribute*. This groups output based only on the first attribute as described above.
- *Do not select Group on First Attribute*—In the layout for each column select *group by* for the individual attributes you wish to report together. This method creates separate groups for each attribute, groups within groups appear.

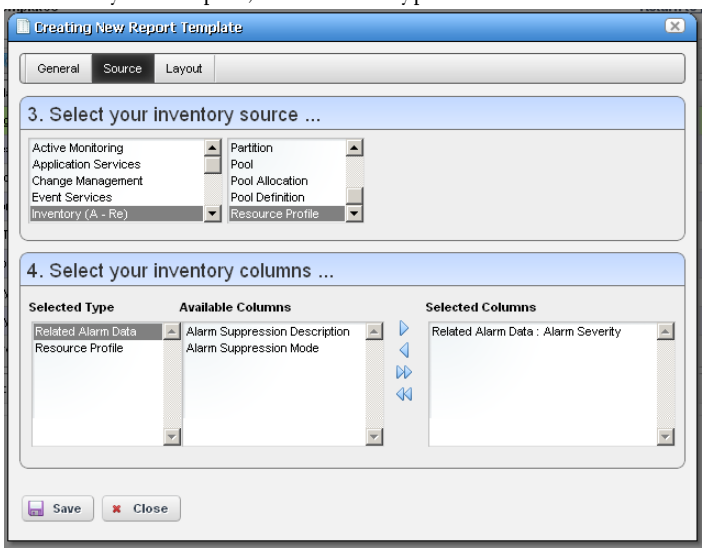
Select both of the above. This method creates a single group using all the columns you have selected in attribute layout and inserts a count for each group.

The Source and Layout tabs are common to all editors.

Summarize Data Only - Generates a report that only shows the raw data, with no column or page headers and no group summaries.

Source

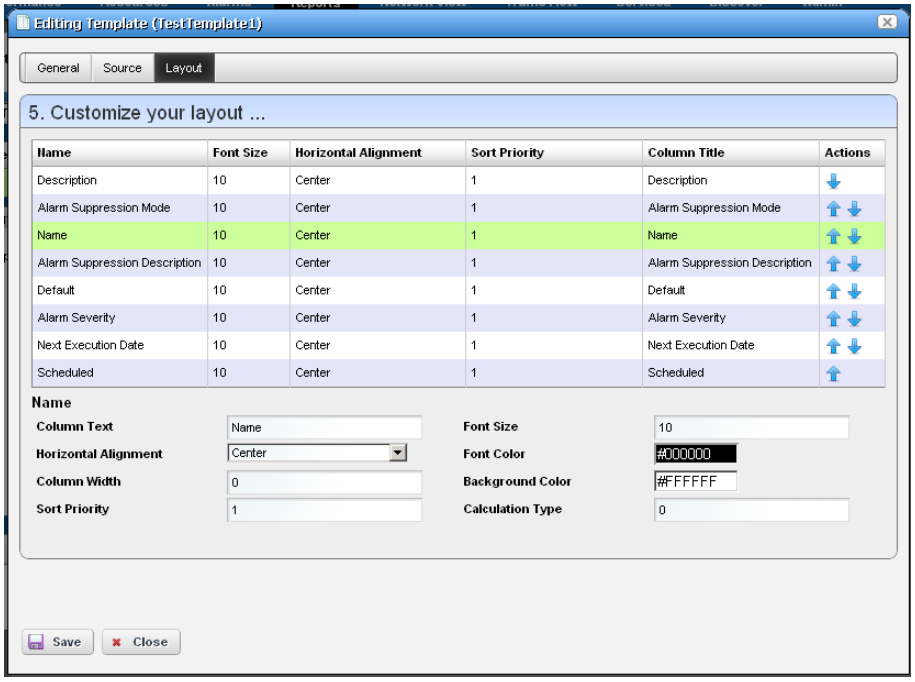
Select the source inventory for a report, and its data types in this screen.



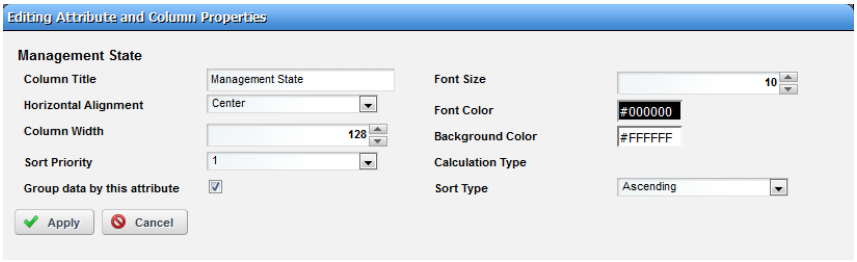
Click the green plus (+) to select the *Inventory Type*. The types of data available for that inventory type appear in the leftmost column in this screen. Click on a *Selected Type* to see its *Available Columns*. Click the arrows to move columns from *Available* to *Selected*. The *Selected Columns* appear in the template's report.

Layout

This tab outlines the column layout for the template.



Click on the up/down arrows on the right of each row to re-order data columns. Click to select a row, and the editor panel at the bottom of the screen appears. It has the following fields:



Column Text—The column label.

Horizontal Alignment—*Right*, *Left*, *Center* (the default).

Column Width—The column width in characters.

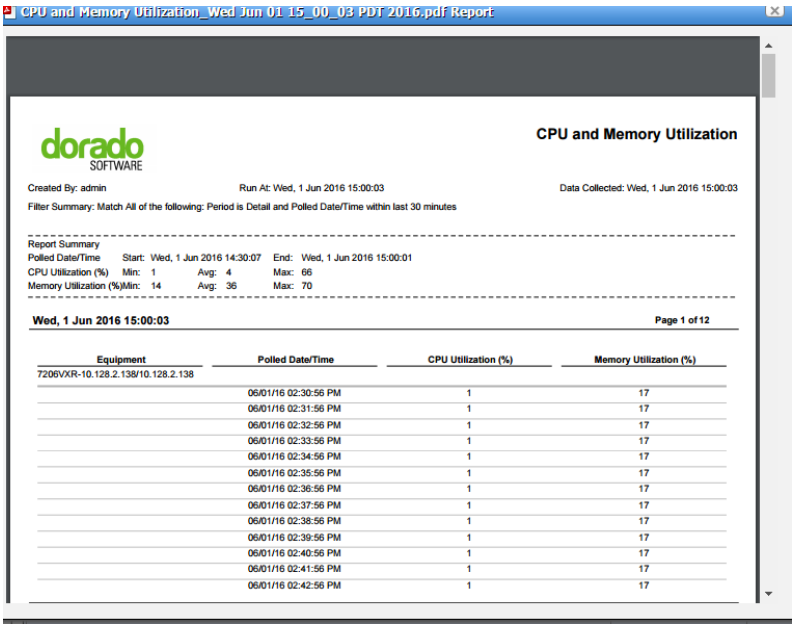
Sort Priority—Configures report sorting. Define the attribute sort order here. You can sort within a sort, so you can sort on Name and then by Location and then by IP Address, and so on. The number configures the sort group, so 1 sorts, then 2 within 1, then 3, and so on.

Font Size—The data's font size.

Font / Background Color—The color for the text/background. Click the field to open a color chooser.

Calculation Type—How to calculate for summarizing the numeric data. Select from the available options, which includes *Average*, *Min*, *Max*, *Sum*, and Min/Avg/Max (which shows each of these together). If Min/Avg/Max is selected for at least one attribute a report summary header

will be created at the top of the report showing the average max and min values for the attribute calculated over all the data rows in the report. The following screenshot shows an example report summary:



Group data by this attribute — If checked, the data will be grouped by this attribute, which means that every distinct value for this attribute will only appear once as a group header and the related data for the other attributes will show rows below this header.

Sort Type — Select ascending or descending.

Click Save to preserve any template you have configured, or Close to close the editor screens without saving.

Settings Page

The Settings page displays the following portlets by default:

- Application Configuration Settings Portlet
- Language Portlet
- Common Setup Tasks Portlet
- Authentications Portlet

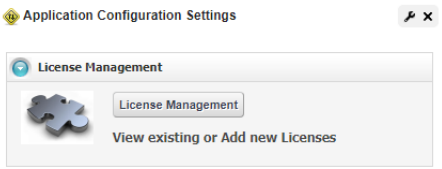
Access the Settings page by clicking Settings from the navigation bar. The Settings menu provides access to the following sub-pages:

Sub-Page	Description
Audit	Displays the Audit Trail Portlet.
Alarm Definition	Displays the following: • Event Definitions • Variable Binding Definitions
Groups & Locations	Displays the following: • Managed Resource Groups Portlet • Vendors Portlet • Locations Portlet • Contacts
Schedules	Displays the Schedule options.
Server Configuration	Displays the Application Server Statistics Portlet.
Site Map	Displays the Site Map Portlet.

Application Configuration Settings Portlet

The Application Configuration Settings portlet provides access the License Viewer window by clicking the License Management button. For details about viewing, registering, and managing your product license, see License Viewer on page 653.

Access this portlet by selecting Settings from the navigation bar.



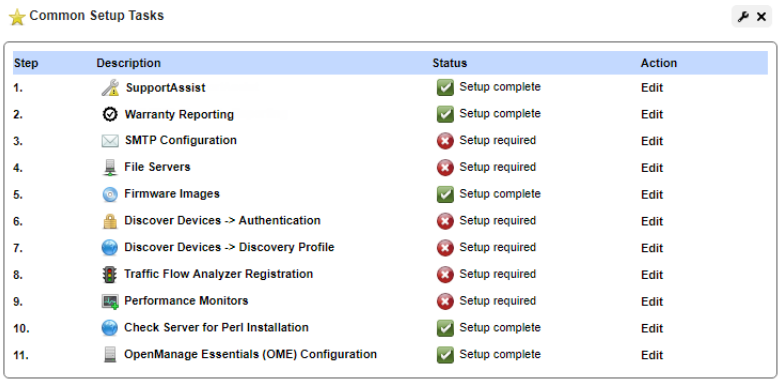
Note that this information provided is based on a default installation before any customization by the customer.

Language Portlet

Common Setup Tasks Portlet

Common Setup Tasks Portlet

By default, the Common Setup Tasks portlet appears on the Settings and Home pages after you sign in. If your package does not display this portlet on these pages and you want it there, click *Add* > *Applications* and put it there.



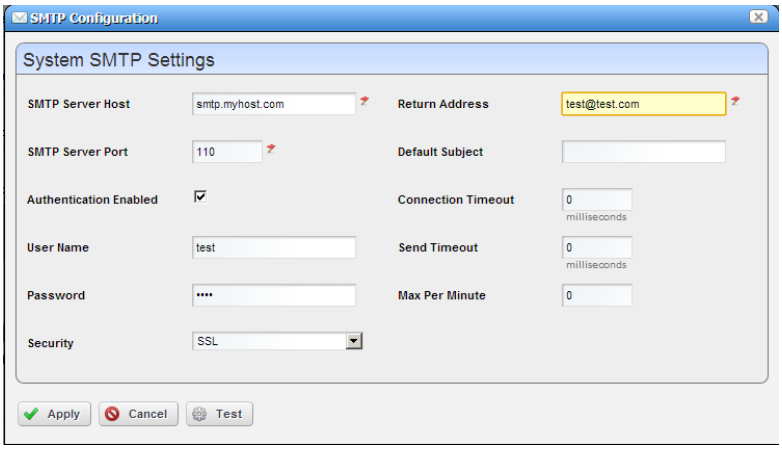
This portlet shows the setup status for the common tasks, such as:

- SMTP Configuration
- File Servers
- Firmware Images

The *Status* column shows whether the setup is complete (check mark) or is required (X). Click the Edit action to modify a task's settings or enable schedules.

SMTP Configuration

You can use OpenManage Network Manager's messaging capabilities to communicate with other users, but if you want to receive e-mails automated by actions like configuration file backups, OpenManage Network Manager must have a mail account. This screen configures the e-mail server so OpenManage Network Manager can send such automated e-mails.



The *Apply* button accepts your edits. *Test* tries them. *Cancel* abandons them and returns to OpenManage Network Manager. This screen contains the following fields:

SMTP Server Host—The IP address or hostname of your SMTP server.

SMTP Server Port—The port for your SMTP server. (Common ports are 25, 465, 587)

Authentication Enabled—Check this to enable authentication for this server. Checking enables the next two fields.

User Name—The login ID for the SMTP server, if authentication is enabled.

Password—The password for the SMTP server, if authentication is enabled.

Security—Enable Secure Sockets Layer (SSL) protocol to interact with your SMTP server, or Transport Layer Security (TLS).

Return Address—The return address for mail sent from OpenManage Network Manager.

Default Subject—Text that appears by default in the subject line of mail sent by OpenManage Network Manager.

Connection/Send Timeout—The time-outs for mail sent by OpenManage Network Manager. If your SMTP server or network is slow, increase the default timeout.

NOTICE

These time-outs are in milliseconds, and have been critical in getting e-mail to work, so do make them long enough to handle whatever latency is normal for your network.

Max Per Minute—The maximum number of e-mails OpenManage Network Manager can send per minute.

Two settings for e-mail servers appear in Control Panel, one in the Control Panel > Portal > Settings Mail Host Names edit screen, and another in Control Panel > Server Administration > Mail. These are for Liferay login and password reminders/resets (see Resetting a Password on page

65). The Portal-based e-mail settings help Administrators limit signups to e-mails only existing in their organization. The screen in that panel provides a list of allowed domain names, if that feature is enabled.

Control Panel > Server Administration > Mail is where to configure the Main server and authentication for routing mail

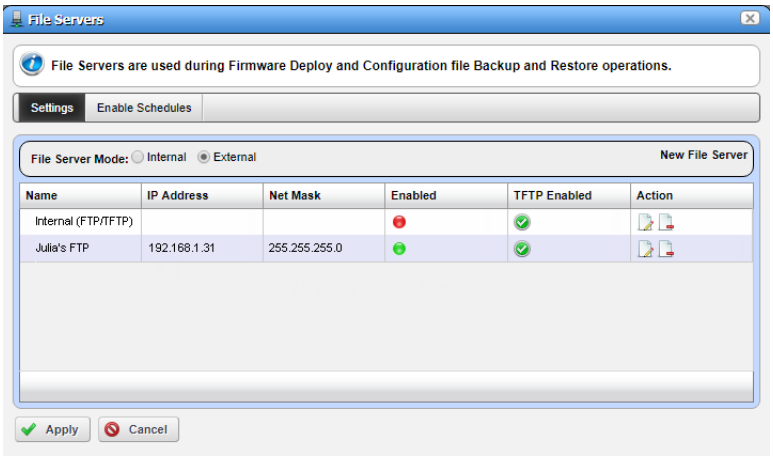
NOTE:

If you require a sender/reply to e-mail address on mail sent, you can configure that with the following property (as always, it's best to override in `owareapps/installprops/lib/installed.properties`)

```
redcell.smtp.returnaddress.name
```

File Servers

The file servers provide FTP connections for retrieving and deploying devices' configuration files, and for deploying firmware updates to devices on your network. See Managing File Servers/Files for a description of the portlet that manages file servers. If you want to configure servers from the *Common Setup Tasks* portlet, a slightly different screen appears when you click *Edit*.



This displays configured file servers. Configure new servers by clicking the *new file server* link in the upper right corner. The editing process after that is as described in External File Server on page 594.

CAUTION:

If you select the internal file server, make sure no external file server is running on the same host. A port conflict prevents correct operation. Either turn off the external file server, or use it as the FTP server. We strongly recommend using the internal file server only for testing, and external file server(s) for production.

OpenManage Network Manager selects the file server protocol for backup, restore or deploy based on the most secure protocol the device supports.

Firmware Images

Use this screen to copy firmware images into the OpenManage Network Manager database. This opens an editor like the one described in Firmware Image Editor on page 588. Refer to Managing File Servers/Files, particularly Image Repository Portlet on page 586 for more about using this capability to deploy firmware to devices you have discovered.

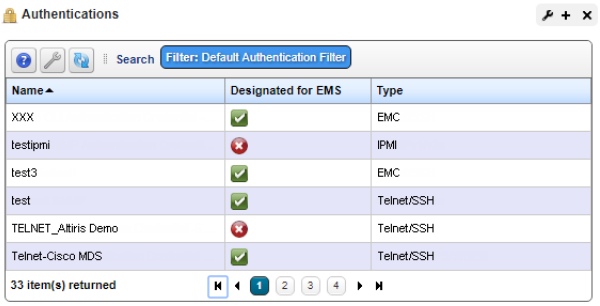
Authentications Portlet

Authentications

The Authentications portlet displays access credentials that let you discover and manage devices on your network.

Settings > Audit Page

By default, this portlet is available from the Settings page.



The *Name* column lists identifiers for sets of credentials, *Designated for EMS* means the credentials are accessible by all users, and *Type* indicates the protocol for that authentication.

NOTICE

If you have multitenancy installed, you can also elect to display a sites column that designates which tenant site owns an authentication.

The following actions are available in the right-click menu:

New / Edit—Opens Authentication Editor, where you can create a new authentication or edit the selected authentication. You cannot change the Authentication Type when you edit an existing authentication.

Details—Displays a reference tree, associated equipment, and the configuration created or altered in Authentication Editor.

Audit—Opens an audit trail viewer for the selected authentication.

Delete—Deletes the selected authentication. If it is in use, an error message appears saying that deletion is not allowed.

Import/Export—Export the selected config file to disk, or import it from disk. You can also import/export a selected configuration file.

Provides the following actions when available for the selected image:

- Import retrieves a file containing XML compliance descriptions. Some imports can come from a URL.
- Export Selection exports the selected description to an XML file.
- Export All exports all descriptions to an XML file.

Click Download Export File to specify where to save the file.

The Import/Export option is useful as a backup or to share descriptors with other projects.

You must import data into the correct portlet. For example, you cannot import event data into the Actions portlet.

If one type of data depends on another, you must import the other data before importing the data that depends on it.

Share with User—Opens the Share with User window where you select the colleague you want to share this assets with and then type your message.

Authentication Editor

You can right-click and select *New* or *Open* to create or modify credentials for your system. You can also *Delete* and *Share with User* from that right-click menu.



The fields that appear in this editor vary, depending on the type of authentication. The *ID* (name) for the authentication is mandatory. If you *Add* an existing authentication, for example to Discovery Profiles Portlet, you can also configure the Management Interface Parameters like *Timeout*, *Retries*, and *Port* used. If you have an authentication that works for multiple protocols (for example SSH or Telnet), you can also select the *Protocol Type*.

NOTICE

Discovery can fail because of network latency / timeout issues. Increasing the timeout or retries for OpenManage Network Manager authentications can circumvent that.

CAUTION:

If you do not get access to the deepest level of authentication—for example the "enable" user—you cannot access all of OpenManage Network Manager's functionality. Also: many devices require more than one authentication—for example SNMP and Telnet / SSH (including that enable authentication).

When attempting to access a device configured with SNMP v3, if you see an error message like `unable to read device serial number for selected credential`, discovery fails. This indicates the SNMP v3 credential is faulty. One common problem: SMNP v3 credentials must be at least eight characters long. Correct it, and discovery and other access should be available. OpenManage Network Manager's SNMP v3 authentications support the following:

- No Auth - No Priv
- Auth with MD5 and SHA digests - No Priv

- Auth with MD5 and SHA digests - Priv with DES, 3DES or AES128 encryption

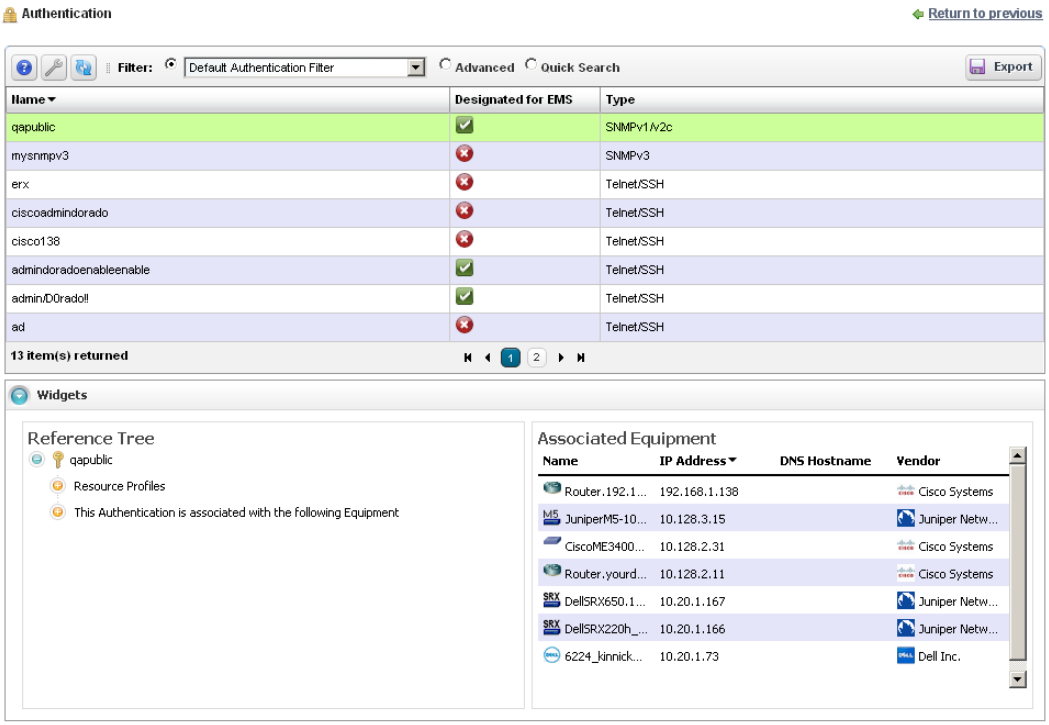
CAUTION:

The standard for SNMP v3 passwords is eight characters or larger. Some devices may accept shorter passwords, but OpenManage Network Manager requires eight characters or longer. **Also**: Traps from an SNMP v3-accessed device do not appear when you change an SNMP v3 login or password on the device or OpenManage Network Manager, unless you resync the device, or until an SNMP monitor polls the device.**Finally:** Rebooting an SNMP v3 device may change the number for the SNMP v3 engine. You must restart application server to pick up this change.

Use the *Equipment* and *User Groups* tabs to associate the authentication you configure here to devices or groups of users.

Expanded Authentications Portlet

The *Settings* button in the expanded Authentication portlet lets you configure column appearance (see Modifying Column Settings on page 85). This offers the same column setup as the summary screen.



Authentication Snap Panel

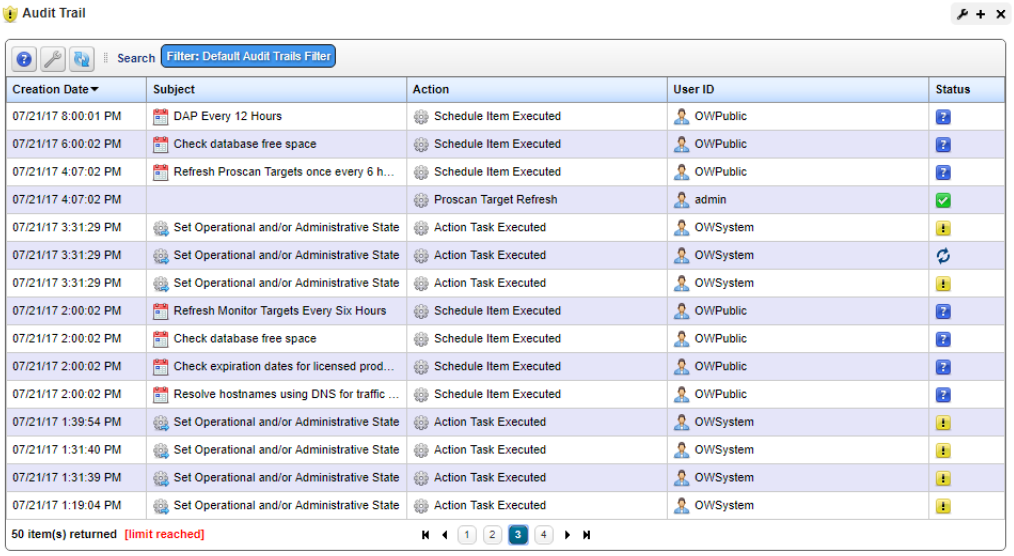
When you select a listed authentication the *Reference Tree* Snap Panel displays a tree of that authentication's connections to Discovery profiles and equipment.

Audit Trail Portlet

Settings > Alarm Definition Page

The Audit Trail summary portlet contains an archive of the Audit Trail/Jobs Statuss message traffic between the OpenManage Network Manager application and monitored devices, as well as the OpenManage Network Manager reaction to failed message transmission.

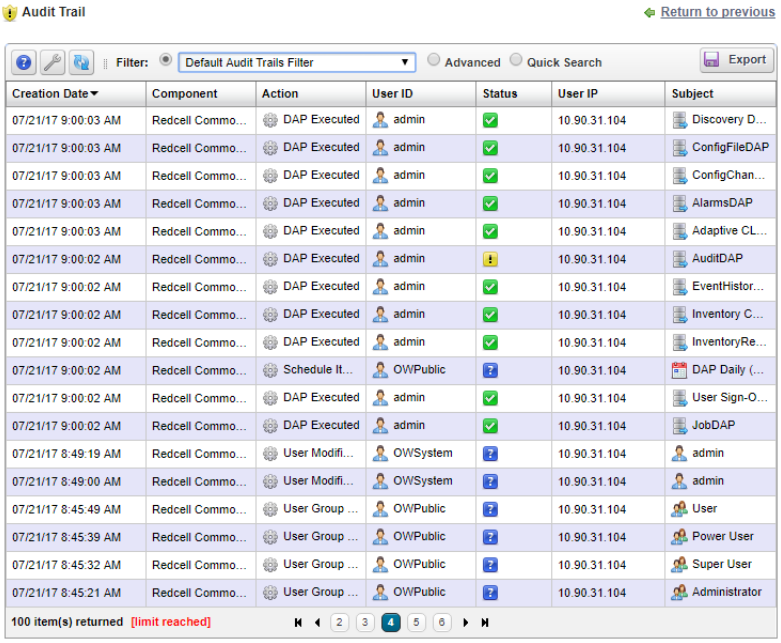
By default, this portlet is available from the Settings page by selecting the Audit menu option.



The *Creation Date*, *Subject*, *Action* (the summary message of the audit trail), *User ID* (the login ID of the user whose actions resulted in this trail), and the status message appears when you hover over the Status field. Right-click an item to *Delete* a message, manage its *Aging Policy*, *View as PDF*, *or Share with User*. See Implementing DAP on page 38 for more about such policies.

Expanded Audit Trail Portlet

When you click the plus (+) in the upper right corner of the summary screen, the expanded portlet appears. Click the *Settings* button to configure the columns that appear in this screen and their order. Filter the screen appearance using the *Advanced Filter* capabilities at its top.



In addition to the summary screen's columns, the following columns are available in maximized vies:

User IP—OpenManage Network Manager creates the Audit Entry for IP Address of the related user. If it cannot acquire the user's IP Address or if the audit entry occurred because of a Scheduled or System event then the IP address is for the related Application Server.

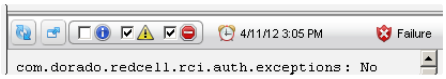
Subject—The equipment at the origin of the message traffic with OpenManage Network Manager.

Right-click an item to provides the same options as the minimized view (Delete a message, manage its Aging Policy, View as PDF, or Share with User).

View Job

The *Audit Job Viewer* displays the audit trail messages in tree form. To see the contents of an individual message that appears in the upper panel, select it and view its contents in the bottom panel. The divider has *Refresh* double-arrow, and screen/arrow icons in the left corner, and an icon indicating the status of the job on the right. Click *Refresh* to clear an old message so you can view a new one.

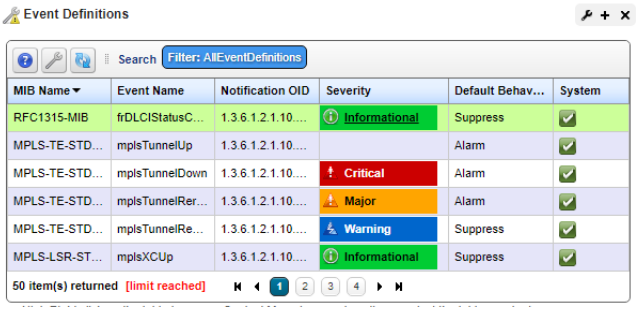
Click the refresh button to check (info, warning, error) filters that limit the types of visible messages. Notice that when you select a message, its date and time appears to the right followed by the status.



Event Definitions

You can define how the OpenManage Network Manager application treats notifications (events) coming into the system. Administrators define event behavior deciding whether it is suppressed, rejected or generates an Alarm. Manage the definitions of events from this portlet.

By default, this portlet is accessed from the Settings page by selecting the Alarm Definitions menu option.



From this portlet, you can configure events that, when correlated as described in Automation and Event Processing Rules on page 512, trigger actions.

Columns include the *MIB Name*, *Event Name*, *Notification OID*, *Severity* for associated alarms, and *Default Behavior*. Alter these settings from the Event Definition Editor. Right-click a selected event definition for the following menu items:

Edit—Open the selected event definition in the Event Definition Editor.

Set Behavior—This lets you select from the following options.

Reject–Every received message is rejected.

Suppress–The message is tracked in Event History and then ignored.

Alarm–The message is tracked in Event History and then processed through the alarm life cycle, which might create a new alarm, increment an existing alarm, or clear an existing alarm.

Set Severity—Set the alarm severity for the selected event, or select the Cleard option.

MIB—This lets you upload a new MIB to your event definitions.

Import/Export—Export the selected config file to disk, or import it from disk. You can also import/export a selected configuration file.

Provides the following actions when available for the selected image:

- Import retrieves a file containing XML compliance descriptions. Some imports can come from a URL.
- Export Selection exports the selected description to an XML file.
- Export All exports all descriptions to an XML file.

Click Download Export File to specify where to save the file.

The Import/Export option is useful as a backup or to share descriptors with other projects.

You must import data into the correct portlet. For example, you cannot import event data into the Actions portlet.

If one type of data depends on another, you must import the other data before importing the data that depends on it.

Share with User—Opens the Share with User window where you select the colleague you want to share this assets with and then type your message.

You can also configure an Aging Policy and View events as PDF in this menu. See Implementing DAP on page 38 for more details.

To see an event's propagation policy, you can view the editor panel described below. See also Understanding Alarm Propagation to Services and Customers on page 119.

Unknown Traps

OpenManage Network Manager normalizes all incoming traps not elsewhere defined as `redcellUnknownTrap` (essentially "none of the above"). When a trap arrives with an OID not in the list of event definitions then the `redcellUnknownTrap` determines its behavior. You can configure OpenManage Network Manager to reject all such traps, suppress them so that they become events or allow them all to become full-fledged alarms.

You can also create event processing rules to handle (suppress, alarm, send e-mail) any such events. See Creating Event Processing Rules on page 95. The `redcellUnknownTrap`'s default behavior is suppress, its default severity is indeterminate. Events and alarms that are unknown still contain the notification OID from the trap. As a formality, `redcellUnknownTrap` has its own notification OID.

The Different Forms of Event and Alarm Correlation

OpenManage Network Manager supports different forms of event and alarm correlation:

- **Stream Based Correlation:** When multiple events occur within the mediation server and there are rules that correlate them with each other so that when a certain kind of pattern is detected (frequency threshold, state flutter), this affects which events the mediation server submits to the application server. You can configure this form of correlation by creating certain types of event processing rules. See Stream Based Correlation on page 486
- **Event to Alarm correlation**: Open alarms are uniquely identified by the source entity and the key bindings. This means that if a new alarm comes in that is essentially identical to an existing open alarm, this will increment the count of the open alarm and also in some cases escalate it or de-escalate it (if the incoming alarm has a different severity level or a different message). This is facilitated by the correlation hash field on each alarm record, which encodes all of the fields relevant for correlation. Note that for key bindings, the data within the binding that is used for correlation depends on how the variable binding definition is configured. If it is configured to correlate By Value then the value within the binding is used and conversely if it is configured to correlate By Index then the index of the OID is used. The index is the last segment in the OID string after the defined OID. For example, if a variable binding definition has an OID of 1.2.3 and the payload of a trap has a variable binding based on this definition with an OID of 1.2.3.55 then 55 is the index of this binding. There will also be a value associated with this binding in the payload of the trap, which is different from the index. See Key Bindings within Correlations on page 502 for more information.
- **Raising / Clearing Alarm Correlation**: When an open alarm with a raising severity (Critical, Major, Minor, or Warning) is correlated with another alarm that was recently created whose severity is cleared, this will then clear the raising alarm (it will no longer be opened). See Event Definitions Correlated Events for Raising / Clearing within Correlations on page 502 for more information.

- Parent / Child Alarm Correlation: In some cases an alarm can cause other alarms to be created and in other cases an alarm can block other alarms from being addressed. In these cases the causing or blocking alarm becomes the parent and the alarms that were caused or blocked are the children. This form of correlation can be performed manually or automatically. For information on manual parent/child alarm correlation, see Parent / Child Alarm Correlation: Alarm Details Panel on page 173. For information on automatic parent child alarm correlation, see Event Definitions Correlated for Parent / Child within Correlations on page 502.

Variable Binding Definitions

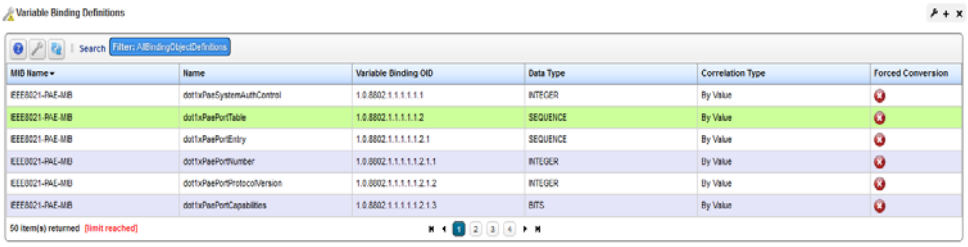
Settings > Groups & Locations

You can define how the OpenManage Network Manager application treats variable bindings that are found within events. Administrators can fine-tune certain aspects of how variable bindings are processed using this portlet.

By default, this portlet is available from the Settings page by selecting the Alarm Definitions menu option.

You might need to edit a variable binding definition if any of these scenarios occurs:

- Alarm to event correlation is not working properly for events/alarms based on a certain event definition - In this case, you might need to find which variable bindings are within the event and change the Correlation Type for one or more of the variable binding definitions. This might then correct the correlation issues for new events and alarms based on the same definitions.
- The message within an alarm is not descriptive enough - In this case, you might need to find which variable bindings are within the event definition upon which the alarm is based and then add latent mined variable bindings so that new alarms based on these definitions will include more information.
- The message within an alarm is unreadable (i.e. it shows up as hexidecimal code) - In this case, you might need to find the which variable bindings are within the event definition upon which the alarm is based and then set it to perform Forced Conversion.

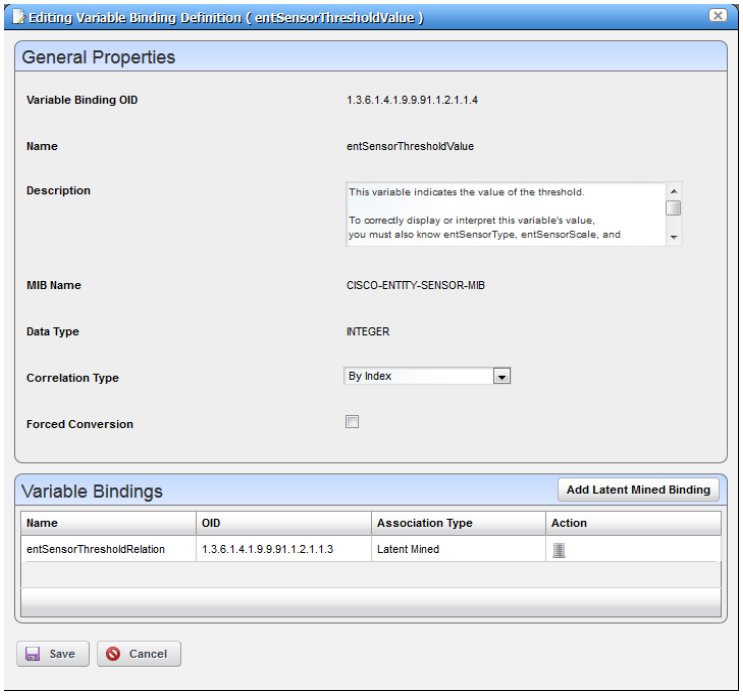


Columns include the *MIB Name*, *Name*, *Variable Binding OID*, *Data Type*, *Correlation Type*, *and Forced Conversion*. See Variable Binding Definition Editor for how to alter these. Right-click a selected variable binding definition for the following menu items:

Edit — Open the selected variable binding definition in the Variable Binding Definition Editor.

Variable Binding Definition Editor

This editor lets you modify variable binding definitions



It has the following fields:

Name — A text identifier for the variable binding.

Variable Binding OID — Unique identifier for the variable binding.

MIB Name — The MIB with which this variable binding is associated.

Data Type — The data type, as defined in the MIB.

Correlation Type — The way that variable bindings based on this definition should be correlated. You might need to change this value if certain types of events and/or alarms do not correlate correctly for your system-for example the clearing alarm does not clear the initial raising alarm-then you can edit one or more of the variable binding on the Message Template tab of the event definition. The possible values for this attribute are: *By Value*, where all bindings have both an OID and a value, the value is used to correlate (this is default), and *By Index*, e.g. OID of 1.4.5.3.4389.334 where no binding exists with this exact OID but 1.3.5.3 does exist and is configured this way will use the remainder of the string (4389.334 in this example) to correlate. The correlation value that is extracted from the binding (whether By Index or *By Value*) is only relevant if this particular binding is configured as a key binding within the event definition (see Event Definitions on page 633 for an explanation of key bindings) and this is used for event to alarm correlation, not other forms of correlation (see Correlations on page 502 for an explanation of the different forms of correlation).

Forced Conversion — Indicates whether or not forced conversion should be applied to the data within the variable bindings that are based on this definition. This is false by default. If this is set to false, then it is possible that variable bindings based on this definition will have data that does not conform to the data type it is supposed to have based on what is stated in the MIB. For example,

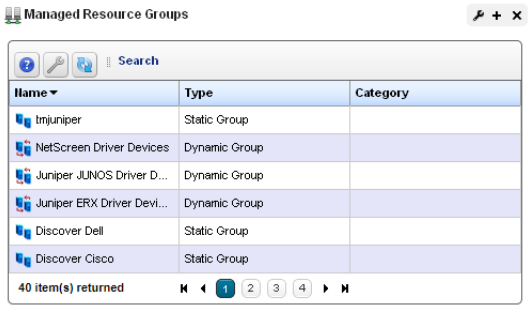
the MIB might say that a certain variable binding is supposed to be an integer, but there could nonetheless be a device that sends data based on this definition as a string. If this is set to true, then this will enable a conversion mechanism so that it will ensure that the data will conform to the data type specified in the MIB.

Variable Bindings — This panel contains a list of additional variable bindings to mine after a trap comes in. The variable bindings present in any SNMP trap is supposed to be specified in the MIB, but sometimes more variable bindings are needed to so that the resulting alarm message contains the necessary contextual information. If more variable bindings are needed, but can only be accessed by using data from one that has already come in then this should be specified here where the variable binding you are editing is the one that is expected to come in the payload of the trap and the binding listed within this panel are then mined using the index of the binding that is based on the definition you are editing. You can push the button *Add Latent Mined Binding* and select a binding from the popup and add it to this list. After you save this screen, the bindings you add will show on the Message Template tab of any event definition that contains this binding in its trap payload based on the trap definition as specified in the MIB. Note that any bindings added to this list are latent mined, meaning that they are only mined during alarm correlation. The data from these bindings can be used in the message template and/or key bindings of the respective event definition, but latent mined bindings cannot be used in filters, nor for extensions, and nor for entity lookup. If you would like to use a mined binding for any of those features, you will have to use critical mining rather than latent mining. Critical mined bindings are defined at the event definition level rather than at the variable binding definition level. Please see Event Definitions on page 633 for more information.

Managed Resource Groups Portlet

The managed resource groups make acting on several devices at once more convenient. They also make managing groups of devices possible. The summary screen displays columns describing the group *Name*, *Type*, and *Icon*. Typically a variety of Dynamic Groups come with your package. For example, Discovered devices are all added to *All Devices* automatically.

By default, this portlet is available from the Settings page by selecting the Groups & Locations menu option.



You can also right-click to do the following:

New—Lets you make either a Static Group (one in which you select devices) or a Dynamic Group (one in which a filter selects devices). See details of these screens below.

Edit—This opens the same editors as *New*, populated with the information for the selected group.

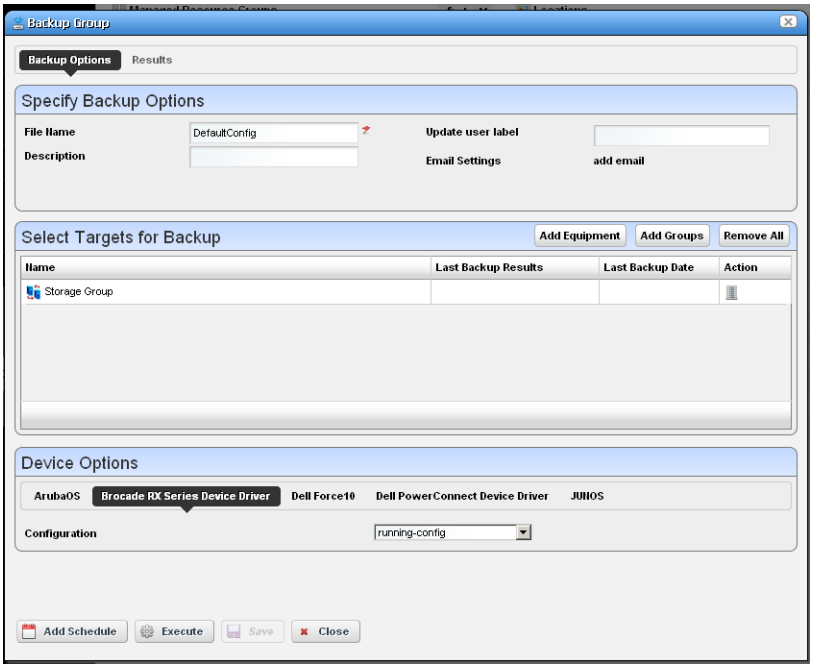
Edit Resources—Lets you edit resources associated with the selected group like its location, contact, or whether to manage it by hostname.

Visualize—Displays a topology map of the selected group. See Using Visualization Tools for more.

Actions—Select from a sub-menu of actions available for the group. This includes Adaptive CLIs. Select from a sub-menu of Adaptive CLI.

If you want the target to be a group of devices, Ctrl + click the target devices before your right-click to invoke an action, or right-click in the Groups portlet and select *Actions* there.

File Management > Backup, Restore, Deploy—Lets you call on OpenManage Network Manager's NetConfig configuration file backup, restore and deploy capabilities. See Backing Up Configurations on page 151 for an example of the steps this follows. See also File Management Menu on page 582 and more about deploying updates to the OS for the selected resource group. See Deploying Firmware on page 154 for details.



When you select a group backup, and the group contains devices of several types, the *Device Options* panel displays a tab for each device type. Select the backup parameters there before executing or scheduling backup.

NOTE:

Some devices merge rather than replace configurations when you select Restore. (Cisco XR, for one)

NOTICE

You can tune resources consumed by processes like backup or resync. See How to: Tuning Application Features' Performance Impact on page 73

Link Discovery—Discover links between members of the selected group, and others. See New Link on page 532 and Link Discovery on page 533 for details.

Resync Resources—Queries the devices in the group to update OpenManage Network Manager's database. Resyncing also resyncs alarms on the selected device.

Delete—Remove the selected group from inventory. The devices remain in inventory, but this removes the grouping.

Import/Export—Export the selected config file to disk, or import it from disk. You can also import/export a selected configuration file.

Provides the following actions when available for the selected image:

- Import retrieves a file containing XML compliance descriptions. Some imports can come from a URL.
- Export Selection exports the selected description to an XML file.
- Export All exports all descriptions to an XML file.

Click Download Export File to specify where to save the file.

The Import/Export option is useful as a backup or to share descriptors with other projects.

You must import data into the correct portlet. For example, you cannot import event data into the Actions portlet.

If one type of data depends on another, you must import the other data before importing the data that depends on it.

Share with User—Opens the Share with User window where you select the colleague you want to share this assets with and then type your message.

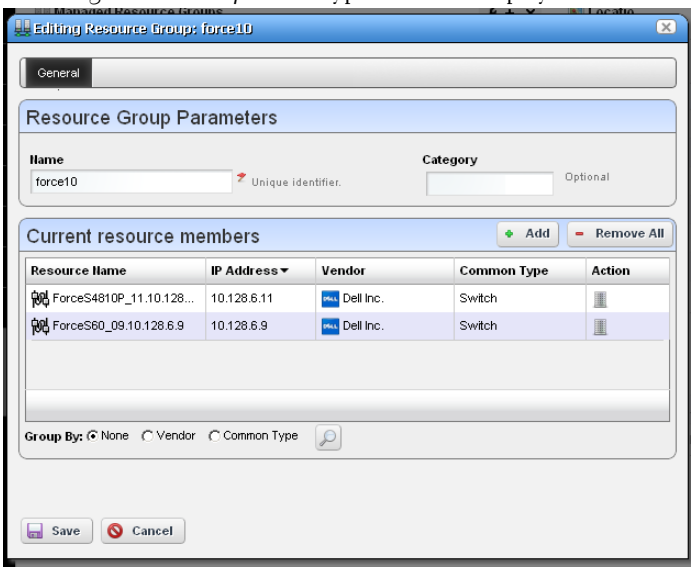
OpenManage Network Manager does not supports static groups that include members retrieved by (dynamic) filters. You can configure membership with dynamic resource groups that include group memberships as filter criteria. For example you can create a filter for members of ResourceGroupABC or members of ResourceGroupXYZ.

Expanded Managed Resource Groups

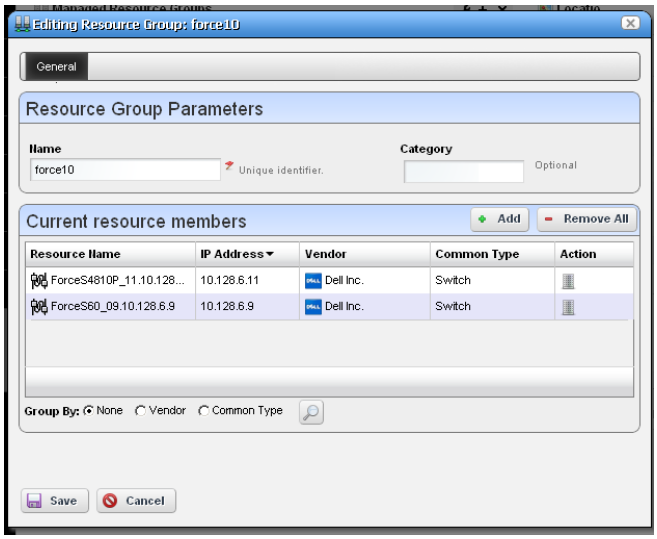
The expanded Managed Resource Groups screen lets you see the summary screen's groups with a Reference Tree snap panel that displays a selected group's connection to its devices and any assigned monitors.

Static Group

Selecting *Static Group* as the type to create displays a selector screen where you can *Name* and



select a *Category* for the group, then search for available resources with a filter. Click *Apply Filter* after you have configured it, and a list of devices fitting its criteria appears. Select device(s) and click *Add Selected*, or simply click *Add All* to add the entire list to your static group. Notice that you can continue to re-use this filter to list devices, and continue to select them.

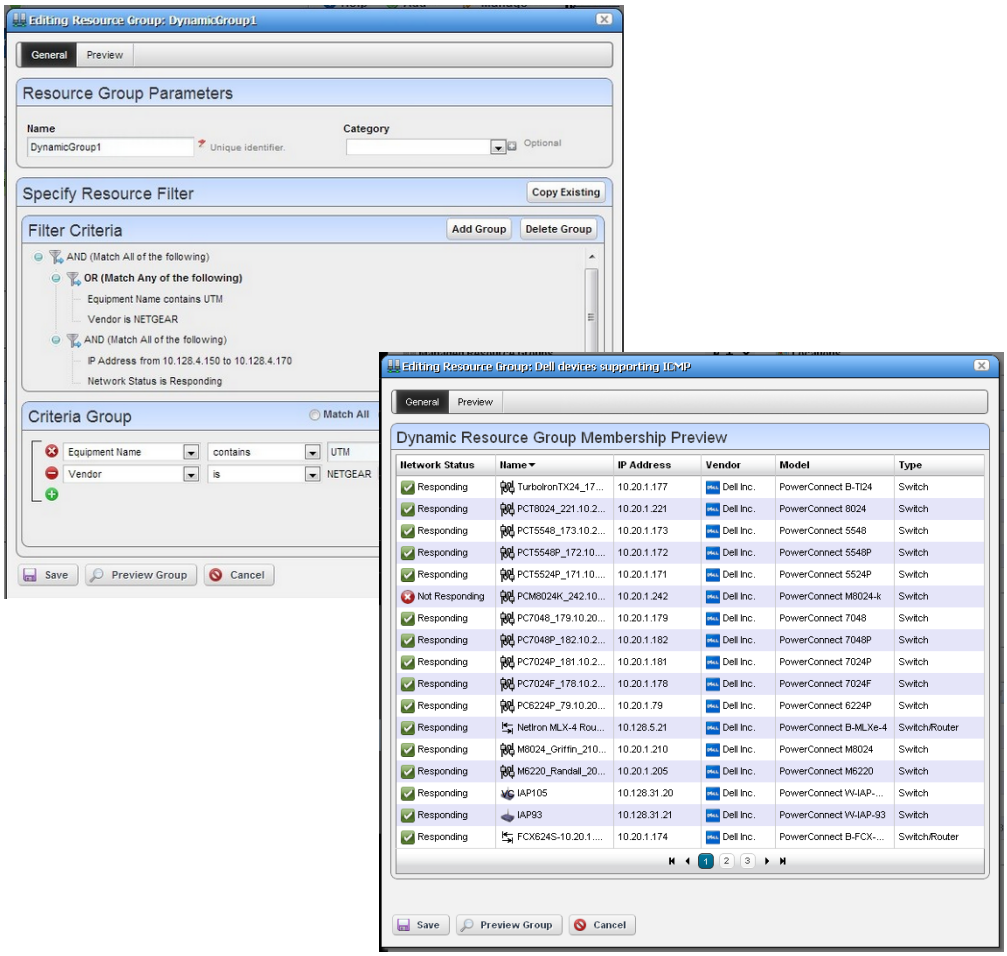


When you select a device, it no longer appears listed. When you click *Done* the subsequent screen displays all devices you have selected. You can click *Add* on this screen to return to the previous screen (or *Remove All* to delete the listed devices from the group). At the bottom of this screen, you can also elect to group devices by *None*, *Vendor* or *Common Type* (Switch, Router, and so on). These last two create "trees" with nodes for each vendor or type. You can also click the magnifying glass to search through listed devices. Clicking *Remove All* removes all devices in the group.

Click *Save* to preserve the group you have configured.

Dynamic Group

In contrast to Static Groups, Dynamic Groups do not let you select individual equipment. You

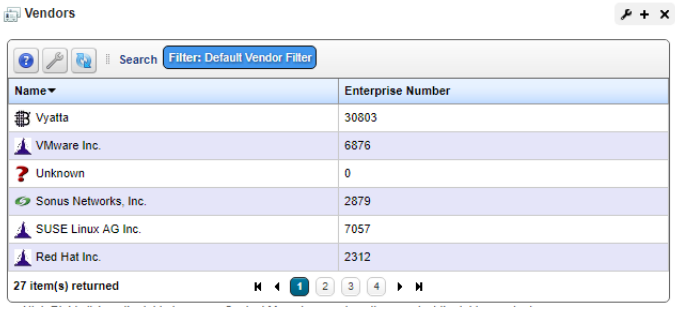


simply configure a filter, and OpenManage Network Manager creates the group on the fly. After you enter the *Name* and *Category* for the group, create the filter. To see what the group would look like, click *Preview Group*. This opens the *Preview* tab, concealing the *General* tab. To return to *General*, click that at the top of the screen. Click *Save* to preserve the group configuration, or *Cancel* to exit without saving.

Vendors Portlet

The Vendors portlet displays the available vendors for network resources.

By default, this portlet is available from the Settings page by selecting the Groups & Locations menu option.



Right-clicking a row lets you do the following:

New / Edit—Opens the Vendor Editor where you can configure or re-configure a vendor.

Details—Displays a panel showing the alarms, registered models, and identifiers for the selected vendor.

Visualize—See a topology of the network filtered to display only the selected vendor, see Using Visualization Tools

Import/Export—Export the selected config file to disk, or import it from disk. You can also import/export a selected configuration file.

Provides the following actions when available for the selected image:

- Import retrieves a file containing XML compliance descriptions. Some imports can come from a URL.
- Export Selection exports the selected description to an XML file.
- Export All exports all descriptions to an XML file.

Click Download Export File to specify where to save the file.

The Import/Export option is useful as a backup or to share descriptors with other projects.

You must import data into the correct portlet. For example, you cannot import event data into the Actions portlet.

If one type of data depends on another, you must import the other data before importing the data that depends on it.

Delete—Delete the selected item. *Caution:* such deletions can impact anything else referring to what you are deleting.

This screen has the following columns:

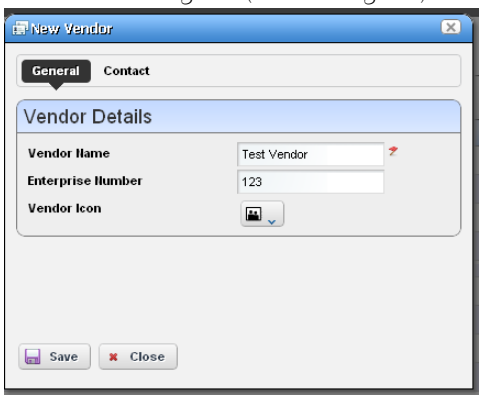
Vendor Icon—The icon for this vendor.

Enterprise Number—The enterprise number for this vendor.

Vendor Name—The name for this vendor.

Vendor Editor

This editor configures (or re-configures) vendors.



It has the following fields:

General

Vendor Name—A text identifier for the vendor.

Enterprise —A numeric identifier for the vendor.

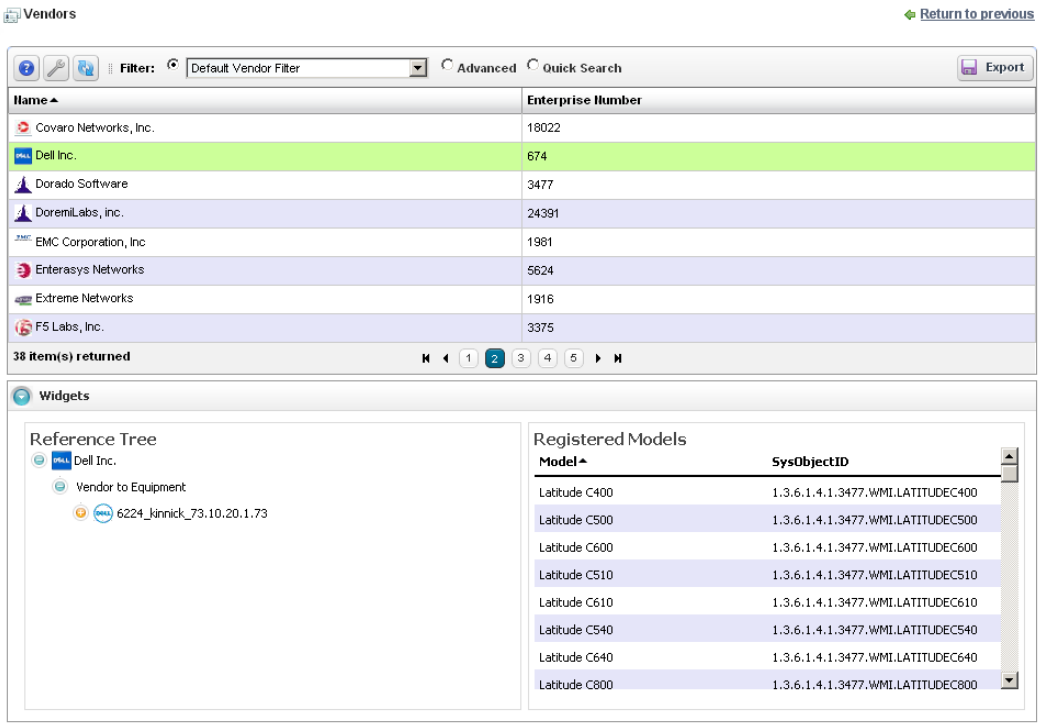
Vendor Icon—Select an icon from the pick list.

Contact

Click the *Add* button to select from contacts in OpenManage Network Manager to associate with this vendor. See *Contacts on page 647* for instructions about configuring contacts.

Expanded Vendor Portlet

When you expand the Vendor portlet, besides sharing you can also click *Settings* to configure the columns that appear here (see Modifying Column Settings on page 85). This screen has the same columns and menu items available as the summary screen.



Vendors Snap Panel

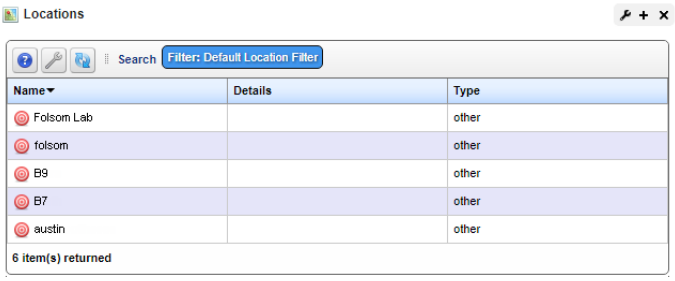
The snap panel displays the icon for the selected vendor.

Locations Portlet

Locations

The Locations portlet displays configured locations in your system.

By default, this portlet is available from the Settings page by selecting the Groups & Locations menu option.



You can right-click to create, modify or remove (*New*, *Open*, *Delete*) the selected location. See Location Editor description below for more about editing or creating locations.

If you select *Visualize*, a map of the selected location's connection to equipment appears. See Using Visualization Tools for more.

This screen has the following columns:

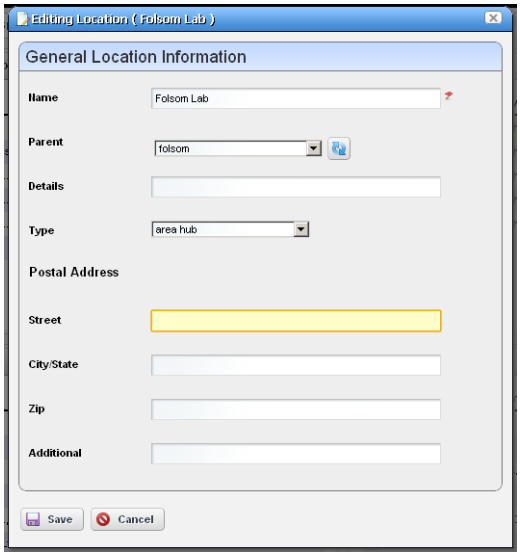
[Icon]—The icon for this location.

Name—The name for this location.

Details—A description for this location.

Type—A designated type for the location.

Location Editor



When you click *New* or *Open*, an editor appears. The *Name* field is mandatory.

Name—A unique name for the Location. If you alter the name of an existing location already in use by existing equipment, the editor creates a new location. If you change the name of a location, this change may take a short period to percolate to all managed objects that use it. You can do this, though.

Parent—The "parent" of this location (the location to which this location is subordinate). Select a Parent Location from the pick list. The maximum number of levels supported is 15.

Details—A text description of the location.

Type—Type of location, as selected from the drop-down menu. Available types are: Area Hub, Customer, National Hub, Other, Provider, Regional Hub, and State.

Postal Address—The *Street*, *City/State*, *Zip* address of the location.

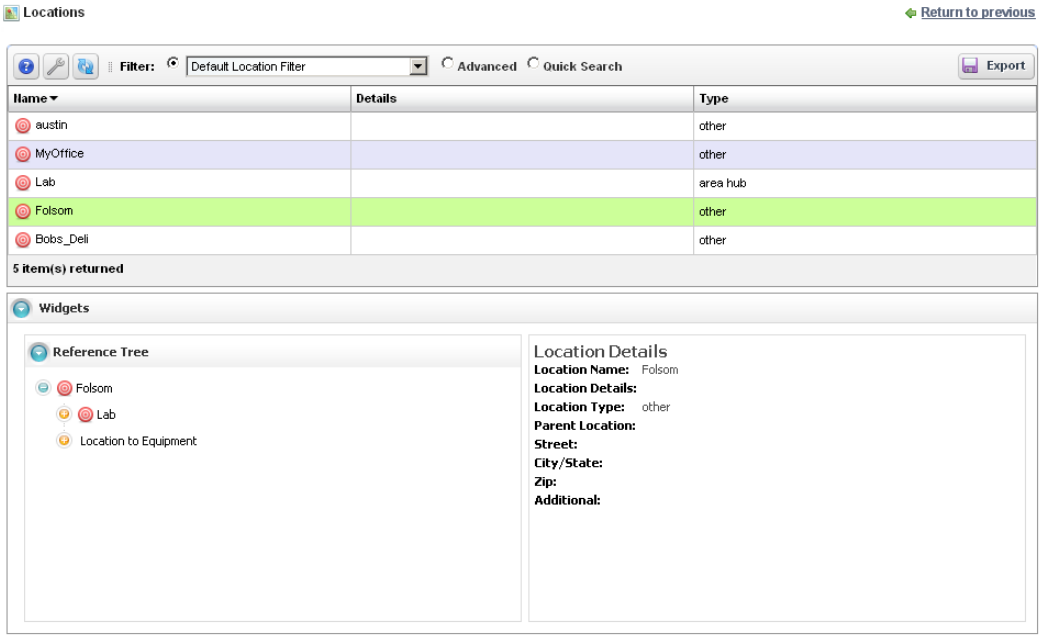
Additional—Any optional notes.

Click *Save* save the Location, or any modifications you have made.

CAUTION:
Deleting locations can impact anything else referring to what you are deleting.

Expanded Location Portlet

The location portlet displays a list of all locations, with Snap Panels to display a selected location's connection to the network and details.



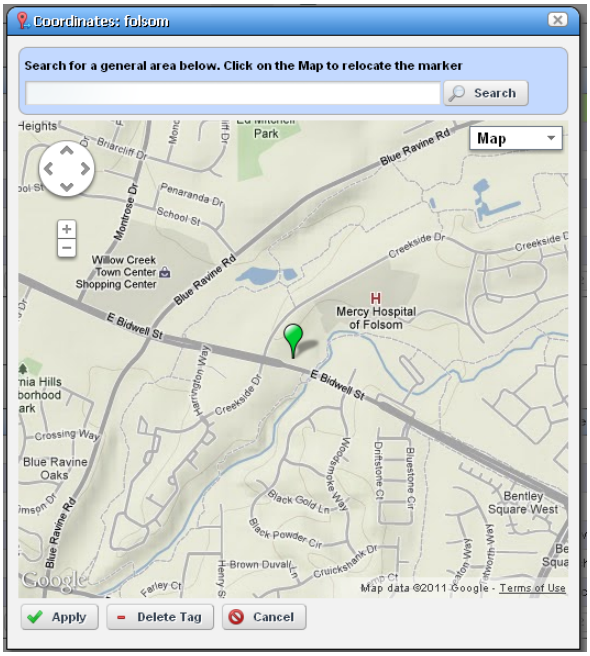
The *New* menu option appears in the expanded location portlet. Click *Settings* to change the column appearance (see Modifying Column Settings on page 85). This has the same columns as Locations on page 644.

Locations Snap Panels

Selecting a location row displays the *Reference Tree* Snap Panel, with that location's connection to containers (see *Container View Portlet on page 510*) and equipment. Click the plus (+) icons to expand the tree. The *Location Details* panel displays what has been configured in the Location Editor.

Tag

When creating a location, OpenManage Network Manager automatically selects the latitude and longitude of the address entered for a location. Tag a location by right-clicking it in the Locations portlet.



The location created by default is the address entered in the Locations editor. You can also enter the address in the Search field, or click and drag the marker that appears on this screen. Click *Apply* to accept the re-location. A *Delete Tag* button appears when you have created a tag, and lets you remove it. *Cancel* closes the screen.

NOTICE

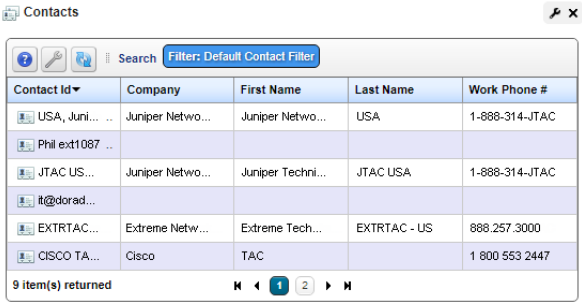
You can zoom in or out on the displayed map with the + and - buttons in the upper left corner of this screen.

Contacts

Settings > Schedules Page

The Contacts portlet displays available contacts for your system. There is no expanded version of this portlet, but you can Ctrl+click to multi-select.

By default, this portlet is available from the Settings page by selecting the Groups & Locations menu option.



You can right-click to act on the the selected contact with the following menu items.

New / Edit—Displays the Contacts Editor, where you can create new contacts or alter existing ones.

Details—Displays a screen with contact-associated alarms, and the information entered in Contacts Editor.

Delete—Delete the selected item. Caution: such deletions can impact anything else referring to what you are deleting.

Because of its simplicity, this portlet does not have an expanded version, so no plus (+) appears in its upper right corner.

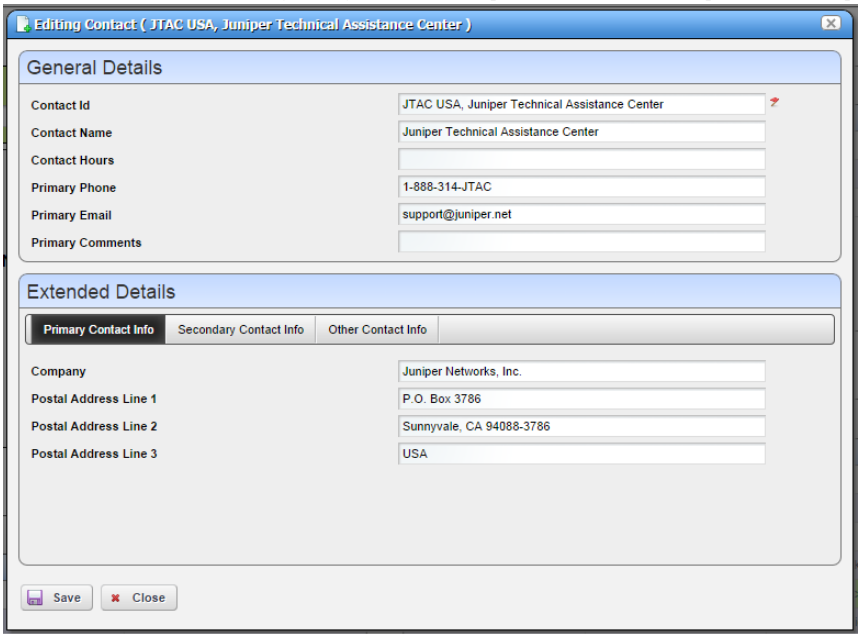
OpenManage Network Manager only retrieves Contact and Location information on initial discovery. You can modify these once the resource is under management, however doing so will not modify any system information on the device.

NOTE:

You can import contacts to Multitenant domains with a command line importer. The command is `importcontacts`. This script is in the `owareapps/redcell/bin` directory. It takes the import file name as a parameter. The domain must exist before it can import contacts, and it generates an error if the contact specifies no domain, or if the domain does not exist. The required domains should exist in the OpenManage Network Manager system before import occurs. Example XML files (with the <customer> tag for domains) are in owareapps\redcell\db.

Contacts Editor

This editor has several panels where you can enter contact information (*Name*, *Address*, *Phone*, and so on). Click the tabs at the top of this screen to move between the panels. The *Contact ID*, a unique identifier for the contact in your system, is a required field at the top of the first page.



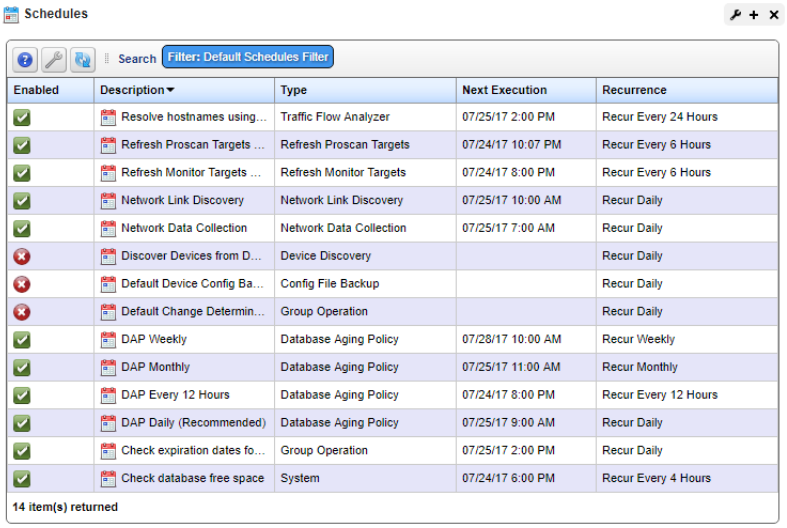
Click *Save* to preserve your new or modified contact information. Click *Cancel* to leave the contact unmodified.

Schedules Portlet

You can view and modify schedules in the *Schedules* portlet, or the Expanded Schedules Portlet.

Settings > Server Configuration Page

By default, the Schedules portlet is available from the Settings page by selecting the Schedules menu option.



This displays the *Enabled* status, a *Description*, the *Type* of schedule, its *Next Execution* and *Recurrence* in columns. You can do the following by right-clicking a scheduled item, and selecting the appropriate menu item:

New—This lets you initiate new schedules for a variety of actions, selected from a sub-menu. The subsequent screen's appearance depends on the action selected. See Managed Resources on page 454 for more about available actions. See Scheduling Actions on page 307 for the details of scheduling actions that require parameters. You can also schedule Action Groups, Alarm Suppression, Config File Backup/Restore, execution of a Database Aging Policy, and OS Image Deployment.

Action Groups are named combinations of actions. The subsequent editor screen lets you configure Actions, their targets, and the order in which they execute.

Edit—This appears for an activity-based scheduled items. It opens the activity editor, and lets you modify the activity's data/properties and schedule parameters.

To edit an existing schedule for an already scheduled action like a Discovery Profile, just right click the item in its portlet and select *Schedule*. This displays the schedule information for the discovery profile and lets you make modifications.

NOTICE

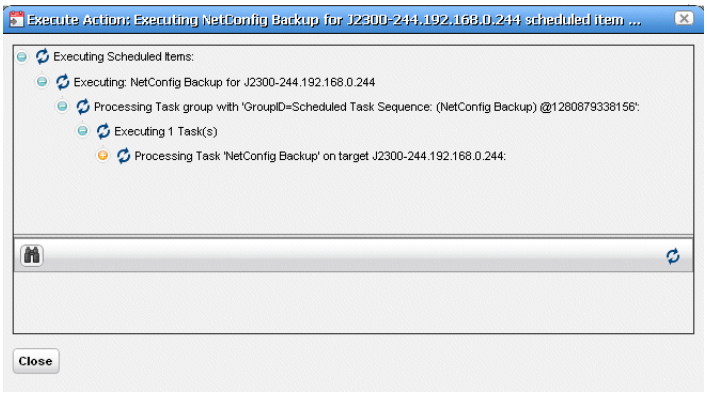
You can also schedule new actions from the portlet that ordinarily executes them, for example Discovering Resources on page 138.

Delete—Deletes the selected scheduled item, displaying a confirming dialog box.

Enable Schedule—Appears on an already disabled scheduled item so you can change its status. To enable the schedule, you can also edit it and check the *Enabled* check box.

Disable Schedule—Appears on an already enabled scheduled item.

Execute—Executes the scheduled item. If the scheduled item is an activity-based or discovery-profile based scheduled item, an audit viewer appears progress of the selected item.

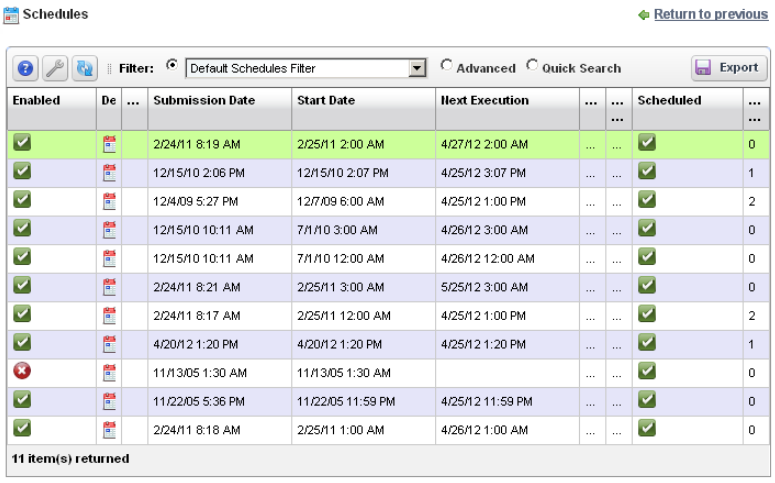


For other types of scheduled actions, a dialog appears saying *The scheduled item(s) has been sent to the application server for immediate execution.* You can monitor its progress from the Audit Trail portlet. (see Audit Trail/Jobs Status on page 689)

If you have OpenManage Network Manager's Change Management/Proscan capabilities installed, you can use Schedules to initiate the Change Determination process. See Change Determination Process on page 344. It is disabled by default.

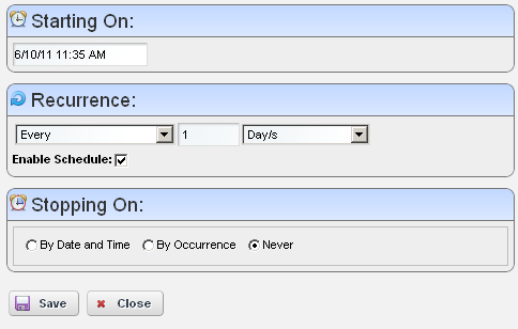
Expanded Schedules Portlet

When you expand this portlet, the additional columns that appear include *Submission Date*, *Start Date*, whether the schedule is still active (*Scheduled*), and the *Execution Count*.



If a check mark appears in the *Scheduled* column, it means the schedule will be executed on next start date. If the schedule has exceeded execution count or passed stop date (if specified), then an "X" appears in the Scheduled column.

To schedule an Action, for example using a discovery profile, right click and select *Schedule*. Alternatively, right-click in the Schedules, select *New* and select what to schedule. The Schedule panel appears, where you can create a new schedule, entering a *Starting On* date and time, and *Stopping On* date and time or occurrence number. You can also configure recurrence in this screen. Make sure you have checked *Enable Schedule* if you want the schedule to be activated.



Once you save the schedule, the action (for example Discovery Profile) also appears in the Schedules Portlet as a scheduled item.

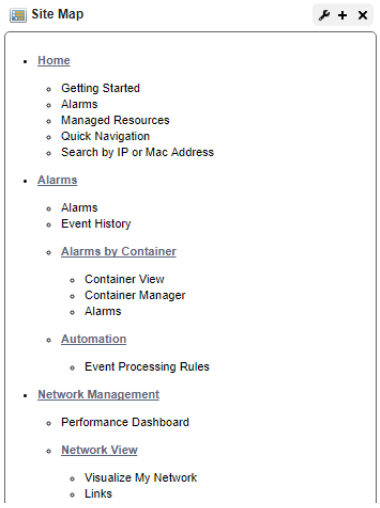
Application Server Statistics Portlet

Settings > Site Map Page

Site Map Portlet

Use the Site Map portlet to see where pages, sub-pages, and portlets are located within your installation. Use your browser's search function to find portlet names within this Site Map.

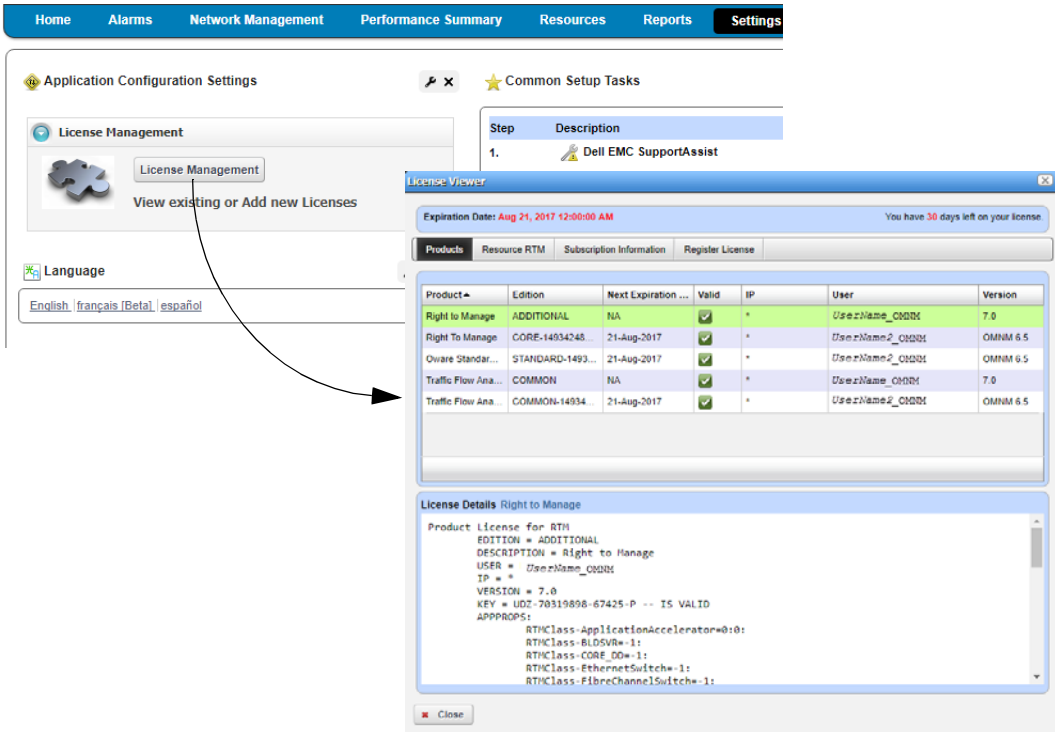
Access this portlet by selecting the Settings > Site Map menu option.



License Viewer

Use the License Viewer window to examine the licenses for your system's capabilities, monitor license expirations, and register a license.

Access the License Viewer window by clicking the License Management button from the Settings > Application Configuration Settings portlet.



The header displays the Expiration Date and how many days you have left on your license. For multiple licenses (such as Application and RTM) that are about to expire, the expiration date is for the license that expires first. Depending on the number of days left, the date and number of days change colors:

- Yellow when 60 days or less are left
- Red when 30 days or less
- Black when 61 days or more

For other methods of getting expiration information, see License Expiration Notification on page 654.

The License Viewer provides access to the following panels by selecting the appropriate tab:

- Product
- Resource RTM
- Subscription Information
- Register License

See Registering a License on page 53 for detailed instructions.

License Expiration Notification

In addition to the expiration information provided in the License Viewer header, the OpenManage Network Manager (OMNM) system includes an alarm warning of possible license expiration (emsAppServerLicenseWillExpireSoon). If your license is about to expire, a **license expiration warning** similar to the following example displays in the Alarms portlet.

```
Application server license will expire in 25 days, on 2017-7-14,0:0:0.0,--
    8:0
```

The time (0:0:0:0) indicates midnight, and --8 hours is the offset from GMT.

When this event occurs, the status bar color changes and displays the following message:

```
Subscription expiration alert: Action required! Your OMNM Subscription is
   about to expire. You have 28 days left before expiration
```

Click the message and the License Viewer, Subscription Information panel opens, where you can start the license renewal process. It also displays the number of days until license expiration.

The alarm color reflects the threshold for the number of days remaining before license expiration:

- 60 days or less: yellow status bar
- 30 or less days: red status bar
- 61 or more days status bar does not change colors

A 0 days left message means that you have exceeded the subscription license expiration. When the **Application license expires**, the following occurs:

- Any data collected up to this point remains stored and **no new data is collected**.
- Status bar does not change colors and does not display a license expired message.
- Most portlets display a message saying they cannot reach the Application server.
- License Management option is still available to register a license when the Application server is down.

  Select Settings > Application Configuration Settings from the navigation bar, click the License Management option, select the Register Product License option, and then click the Select and Register License button. A successfully registered license message is displayed.

When an **RTM license expires**, the following occurs:

- Resources under management and place them in a suspended management state until the number of resource under management meets the RTM license total.
- Suspended resources remain in inventory but cannot be accessed and no alarms are received.
- A resource suspended alarm (resrouceSuspended) is raised for each suspended resource to the user visibility.
- Resources clasified as Other, do not count against the total RTM count.

NOTE:

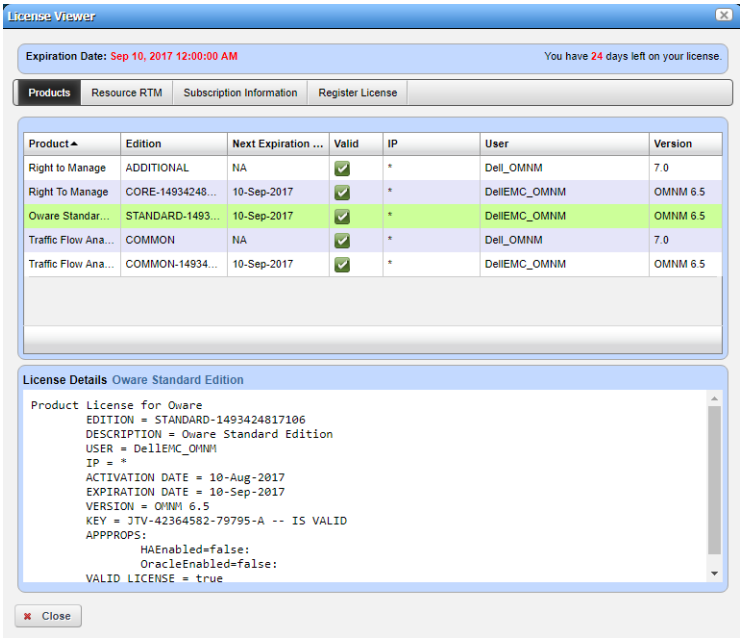
Updating your license clears any expiration alarm and status bar color, but might leave earlier warning alarms in your event/alarm histories. Manually clear the history if you like.

This behaviors applies whether the software is a trial version or yearly subscription.

Product

Use the Product Licenses list to monitor the products for which you have licenses, their expiration dates, and other details about the selected license. The most important product license listed is Oware Standard Edition, which is the Application server license. The Application server requires a valid license to run. All other components depend on a running Application server. If the Application server license expires, you cannot start the server and most applications that you start display a message that the server cannot be reached.

Access this panel by clicking the Products tab from the License Viewer window.



The Product panel provides the following license information.

Column/Field	Description
Product	The product for which you have a license.
Edition	Information useful for support, such as the distinction between core and additional.
Next Expiration Date	The date and time when your license expires. The Application server expiration date controls the Expiration Date information listed in the License Viewer header. The header displays the Expiration Date and how many days you have left on your license. For multiple licenses (such as Application and RTM) that are about to expire, the expiration date is for the license that expires first. If you purchase a new license for a number of days and you have some time left on your current license, what the OpenManage Network Manager system does depends on whether you choose to extend or increase the license during registration. See Register License on page 660 for more details on license behavior.
Valid	An indicator showing whether the license is valid (checkmark) or not (X).
IP	Any IP restrictions (asterisk is unrestricted).
User	The person authorized to use the application.
Version	The license version (not the software).

Column/Field	Description
License Details	The selected registered license details displays information, such as edition, activation date, expiration date, and so on. By default, this field displays information for the first product in the list. To see your license activation date, select the Oware product license and then look in the License Details field for the ACTIVATION DATE parameter. The date is either: • The day you installed the OMNM systerm • The day registered a new license by increasing the license • The day the current license expires if you register a new license by extending your license • A given day if you register a new license from the command line To see your software's Digital Service Tag parameter, select the Oware license and look in the License Details field for the APPPROPS parameter. This parameter is useful in license renewal.

Resource RTM

Use the Resource RTM panel to monitor Right to Manage (RTM) license expiration dates.

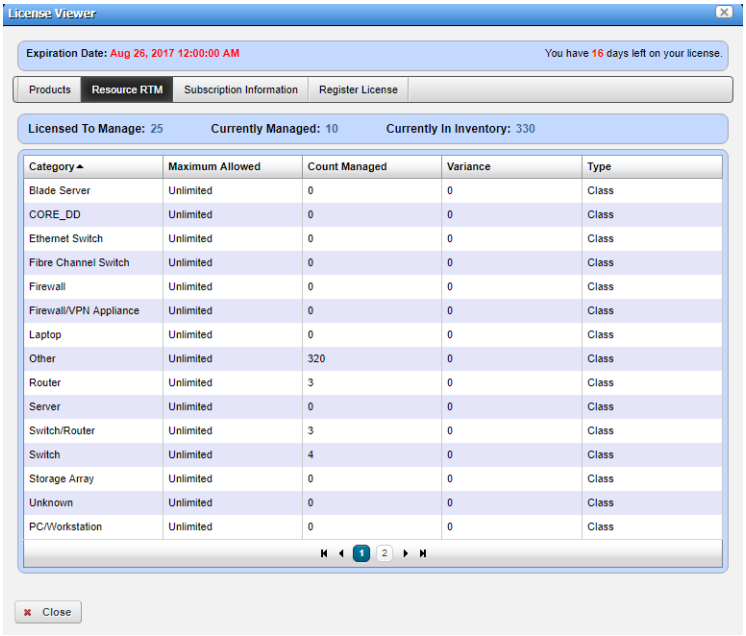
When the RTM license expires, any resource under management exceeding the total RTM count is put into a suspended state based upon the updated date. The most recently accessed resources are the last resources suspended due to an expired RTM license.

NOTE:

If a device's management state is Planned, Decommissioned or Suspended, the device **is not** included in the total RTM count.

When attempting to change a resource's management state, the OpenManage Network Manager (OMNM) system verifies the current RTM licensing to ensure that the RTM license count is sufficient to bring the device back under management. If the RTM licensing check fails, the resource remains in a suspended state. You have the option to suspended another resource to bring a higher priority resource back under management (management state = Normal or Maintenance).

Access this panel by clicking the Resource RTM tab from the License Viewer window.



The Resource RTM panel provides the following license information.

Column	Description
Licensed To Manage	The number of devices you are licensed to manage.
Currently Managed	The number of devices currently under management.
Currently In Inventory	The number of devices in inventory.
Category	In addition to several self-explanatory categories (like Ethernet Switch, Router, and so on), these can include the following: • Other–Any type of device that is not explicitly a current licensed Category. An Other type does not impact the Licensed To Manage for Currently Managed values. **Example:** The OMNM system classifies Wireless Access Points (APs) are Other. These have an unlimited Maximum Allowed count because no license limit exists for the number of Wireless APs that can be attached to a Controller. Only APs attached to a controller are counted for Other. • Unknown–Any device that is successfully discovered with an unrecognized SysObjectId is licensed in the Unknown Category. • Wireless Access Point–The OMNM application licenses any Wireless access point you create by right-clicking in the Managed Resources portlet and selecting the New menu item as Wireless Access Point. The Dell Instant Access Points (IAPs) are also licensed as Category Dell.
Maximum Allowed	The maximum number of managed devices. If *unlimited* appears it refers to device types, not numbers of devices licensed, and indicates no limits exist for classes of devices related to the license row.
Count Managed	The current count of managed devices.

Column	Description
Variance	Licensing can give you a variable number of additional Rights to Manage (RTMs) devices beyond the maximum allowed. For example if *Maximum Allowed* is 100, a variance of 5 allows five additional RTMs. This allows some flexibility to manage additional devices if while awaiting the arrival of additional RTMs. Typically, *Variance* is zero.
Type	The Licensing scheme supports RTM by Class of device. The class of device has an RTM set. Discovery also maps Class type to a device driver. **Note:** The OMNM system does not license by vendor.

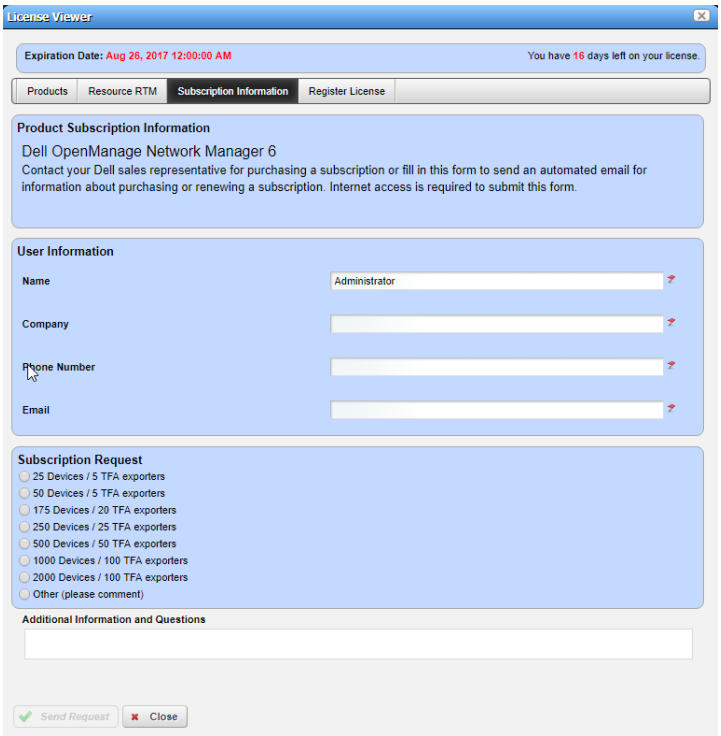
Subscription Information

Use the Subscription Information panel to purchase or renew a subscription license. Enter the relevant information, select the type of renewal, add any additional information or questions, and then click Send Request to request a license.

Once you click Send Request, the information is forwarded to Dell and you are redirected to a Dell order page, where you place an order for a new subscription license.

Access this panel by clicking the Subscription Information tab from the License Viewer window. You can also access this panel by clicking the following message if it appears in the OpenManage Network Manager status bar.

```
Subscription expiration alert: Action required! Your OMNM Subscription is
   about to expire. You have XX days left before expiration
```



The Subscription panel includes the following fields and options.

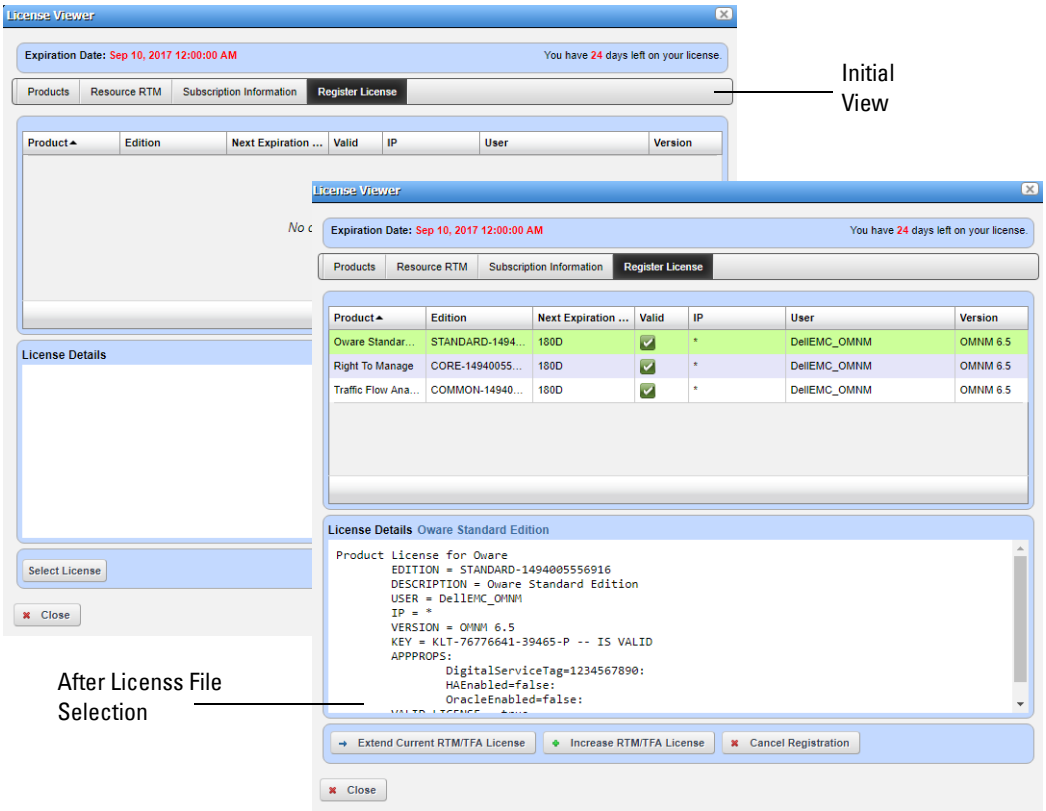
Fields/Options	Description
Name	The user requesting to purchase or renew a subscription.
Company	The company the requestor works for.
Phone Number	The phone number in which to contact the requestor.
Email	The email address in which to contact the requestor.
Subscription Request	The license option you are requisition. Select one of the following: • 25 Devices/5 TFA exporters • 50 Devices/5 TFA exporters • 175 Devices/20 TFA exporters • 250 Devices/25 TFA exporters • 500 Devices/50 TFA exporters • 1000 Devices/100 TFA exporters • 2000 Devices/100 TFA exporters • Other (please comment)

Register License

Use the Register License panel to register your license. When you receive the OpenManage Network Manager (OMNM) software package, it comes with a 30-day trial license for the Right to Manage (RTM) and Application server expiration date. The OMNM installation automatically installs this 30-day trial license.

The expiration depends on the time left on the current Dell EMC subscription license, the length of time for the new Dell EMC subscription license, and whether you are extending or increasing the license.

Access this panel by clicking the Register License tab from the License Viewer window.



The Register License panel includes the following fields and options.

Fields/Options	Description
Product	The product for which you have a license.
Edition	Information useful for support, such as the distinction between core and additional.
Next Expiration Date	The date and time when your license expires. The Application server expiration date controls the Expiration Date information listed in the License Viewer header. The header displays the Expiration Date and how many days you have left on your license. For multiple licenses (such as Application and RTM) that are about to expire, the expiration date is for the license that expires first. If you purchase a new license for a number of days and you have some time left on your current license, what the OpenManage Network Manager system does depends on whether you choose to extend or increase the license during registration. See Register License on page 660 for more details on license behavior.
Valid	An indicator showing whether the license is valid (checkmark) or not (X).
IP	Any IP restrictions (asterisk is unrestricted).
User	The person authorized to use the application.
Version	The license version (not the software).
License Details	The selected registered license details displays information, such as edition, activation date, expiration date, and so on. By default, this field displays information for the first product in the list. To see your license activation date, select the Oware product license and then look in the License Details field for the ACTIVATION DATE parameter. The date is either: • The day you installed the OMNM systerm • The day registered a new license by increasing the license • The day the current license expires if you register a new license by extending your license • A given day if you register a new license from the command line To see your software's Digital Service Tag parameter, select the Oware license and look in the License Details field for the APPPROPS parameter. This parameter is useful in license renewal.
Extend Current RTM//TFA License	This option activates the registered license once the previous license expires. **For example:** If your current Dell subscription is a one-year and 50-RTM license with six months remaining and then you register a new one-year and 50-RTM license with the OMNM system, the system allows managing 50 resources and expires in one and a half years.
Increase RTM/ TFA License	This option activates the registered license immediately. **For example:** If your current Dell EMC subscription is a one-year and 50-RTM license that expires on 12/31/2017 and you register a new one-year, 100-RTM license with the OMNM system on July 1, 2017, the licenses are stacked. The OMNM instance supports 150-RTMs until December 31, 2017, and then 100-RTMs until June 30, 2018.
Cancel Registration	The option to discontinue with the license registration process.

Applications Available for Use

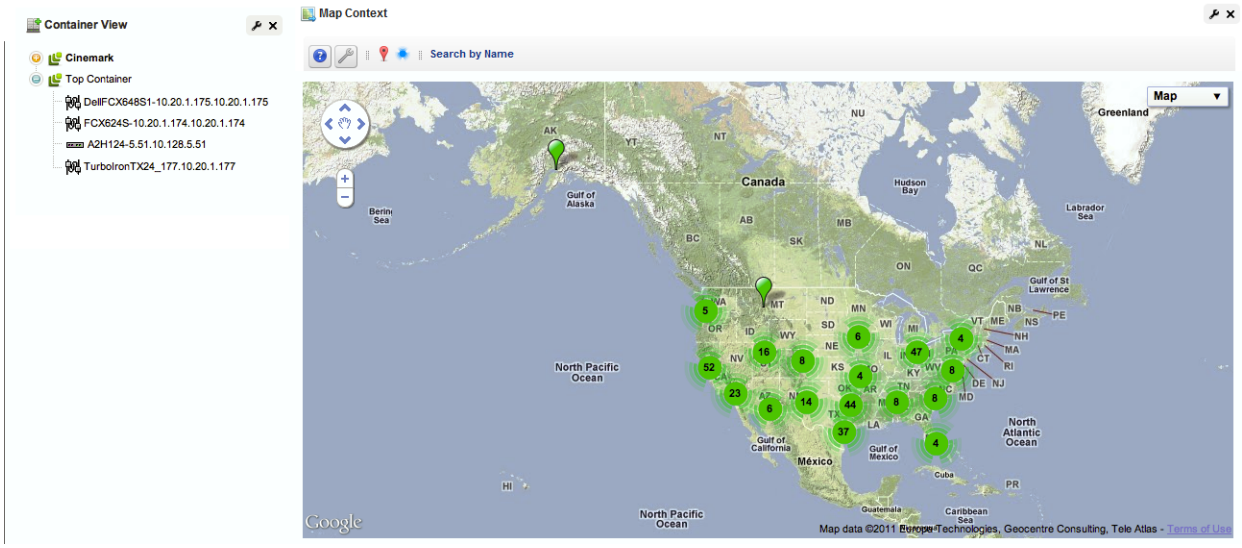
This section describes the following portlets that are not on any page after a fresh installation but can be added to any existing or new page using the Add > Application menu option:

-
- Cards Portlet
-

The applications list displays all available portlets when you select the Add > Application menu option.

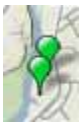
Map Context

In addition to displaying filtered-by-container portlets, you can view discovered devices in the *Map Context* portlet, automatically placed by location.



Notice that you can move the center of the map with the arrows in its upper left corner above the zoom in / out (+/-) buttons. The menu in the upper right corner lets you select a *Map* or *Satellite* views, and fine-tune them to include labels, terrain and so on.

In addition to the *Help* and *Settings* icons at the top of this portlet, you can also *Toggle Marker Style* (pushpins or triangles), *Toggle Marker Clustering* (combine markers into cluster marker when they are near each other), or *Search by Name* for a location. Clustered markers display the number of separate markers combined within them.





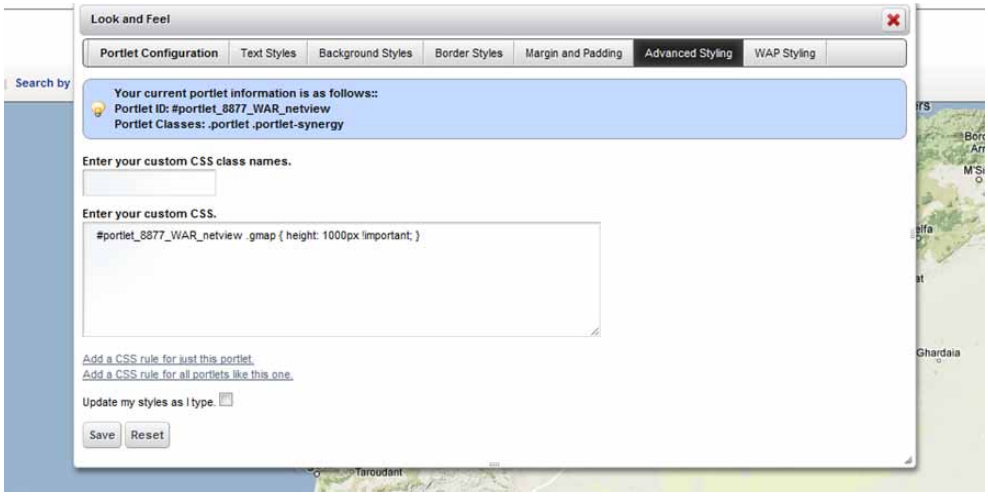
NOTE:

The Search function is case-sensitive. Omit the initial letter if you are uncertain about capitalization for a tagged location.

Clicking the *Settings* icon produces a screen where you can configure the default marker style, whether clustering is enabled, and where you can save the current map boundaries (*Save Current Bounds*), which appear, read-only, below that option.

See General > Entity Change Settings on page 687 for the way to set the summary portlet refresh interval. The default is 40 seconds. This screen also sets the default center of your map.

The page layout controls the width of the map. However you can control the height of the map with the *Look and Feel* configuration in the *Advanced Styling* tab.



Add the following line to the custom CSS settings in this tab:

```
#portlet_8877_WAR_netview .gmap { height: 1000px !important; }
```

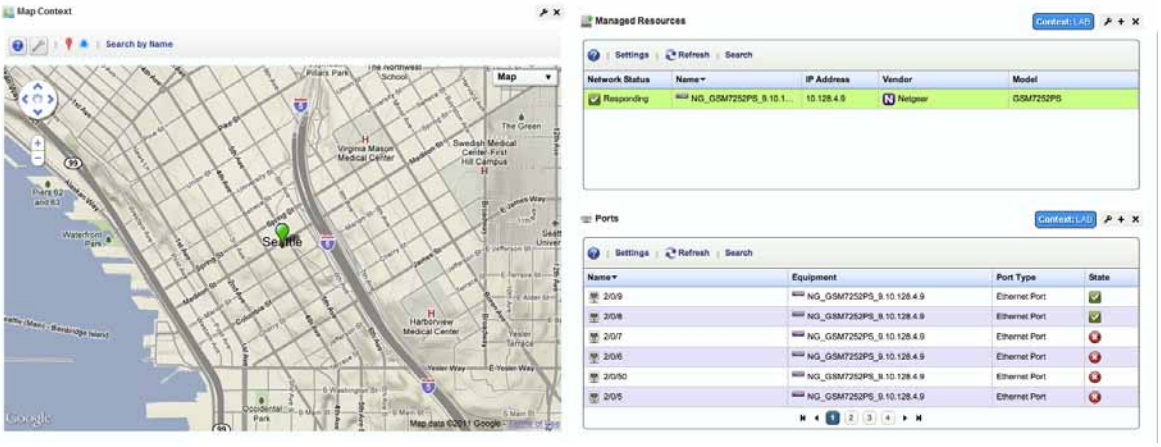
This sets the height of the map context portlet to the configured number of pixels, here, 1000.

Access this tab from the drop-down originating with the word *Map* in the top right corner of the portlet.

Configure mapped container or customer locations with the *Tag* menu item. See *Tag on page 512* for an explanation. See Maps and Containers Together below for more about their joint capabilities.

Map Context without Containers

If a page has no containers then the Map Context can act like a container too. It displays all tagged resources within the system (see Tag *on page 512*). Clicking on a tagged item behaves like clicking a Container, confining displayed resources, alarms, and so on, to those for the selected tag.



Each tagged coordinate is cross-correlated with the Alarm severity table (if there are alarms against it) and its color reflects the current Alarm severity.

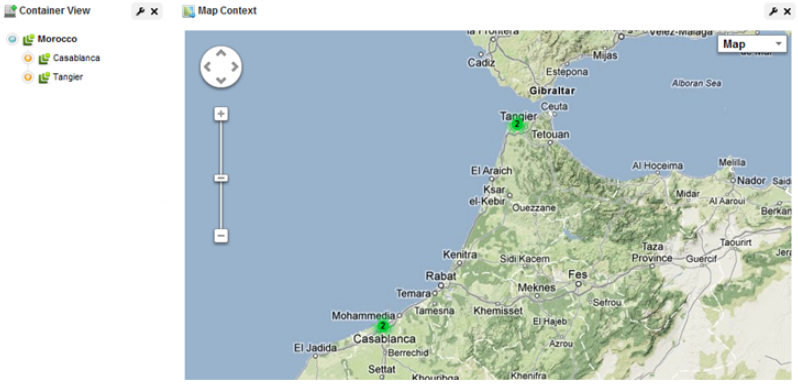
Maps and Containers Together

A map context portlet is in *Standalone* mode when no Container View portlet is on the same page.

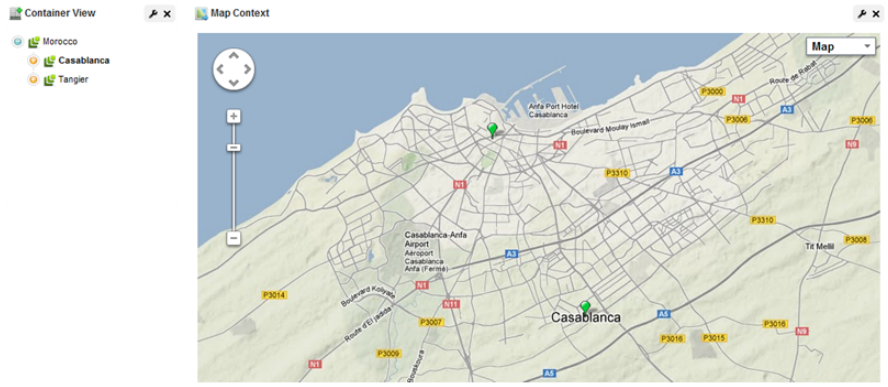


In Standalone mode you can determine exactly what portion of the map appears through the *Settings* option (the wrench icon).

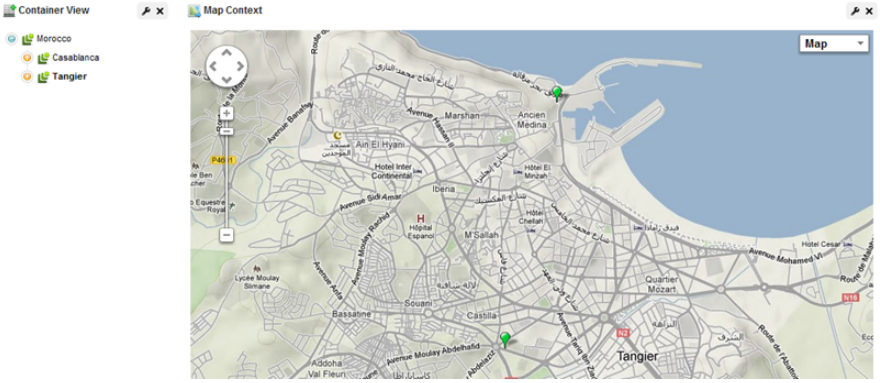
The map context portlet is in *Container Context* mode when a Container View portlet is on the same page. In these Container Context configurations, the Container View determines what appears in the Map portlet, so the Map Context portlet resets its boundaries based upon the geographic position of the selected container's members. For example, you can select a container (Morocco) resulting in two clustered pin for both Casablanca and Tangier.



However if you select Casablanca from the container view the map automatically changes its presentation and boundaries based upon the members of the new selection. The view zooms to the street level in Casablanca.

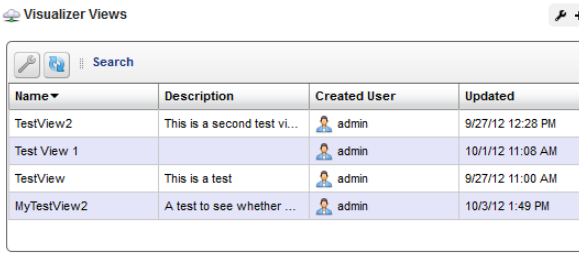


If you select Tangier and map presents the container's sites in a street-level view of Tangier.



Visualizer Views

This portlet displays saved views, and when it is on the same page as the Visualize My Network portlet, filters that portlet so it displays the selected, saved visualization.



Name	Description	Created User	Updated
TestView2	This is a second test vi...	admin	9/27/12 12:28 PM
Test View 1		admin	10/1/12 11:08 AM
TestView	This is a test	admin	9/27/12 11:00 AM
MyTestView2	A test to see whether ...	admin	10/3/12 1:49 PM

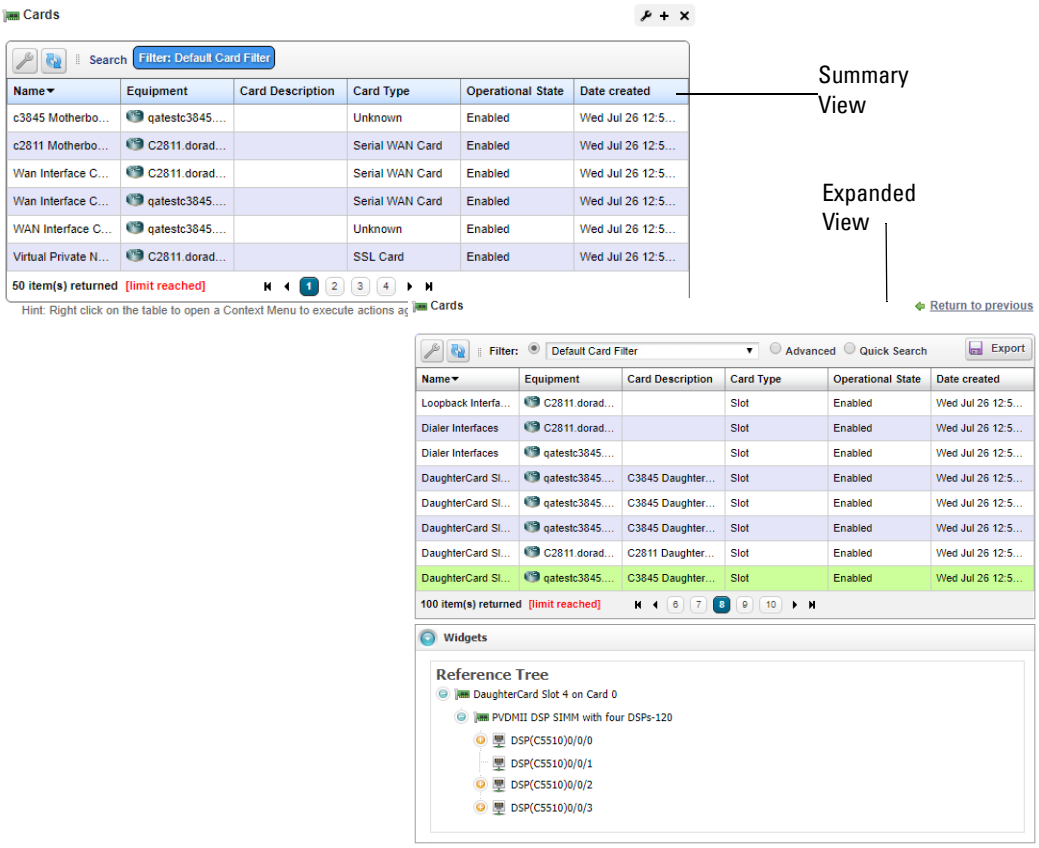
Right-clicking selected views, lets you *Edit* the title of the view, or its description, or *Delete* the selected view.

Cards Portlet

Use the Cards portlet to monitor and manage your discovered card resources.

This portlet is intended for users who are interested in managing their discovered devices.

After installation, this portlet is not from any page. However, you can add it to any page, such as the Resources page by selecting Add > Application, expanding the Resource Management list, and adding the Cards portlet. This portlet has both a summary view and an expanded view. Each view could display different columns and could have the same pop-up menu options available.



Columns

Other than the general navigation and configuration options, the Cards portlets (summary and expanded views) include the following columns. The columns displayed by default are noted.

You can view the value for most of the hidden columns by clicking the Settings tool, selecting the columns tab, clicking Show for the appropriate column, and then applying the change.

Column	Description
Name	A resource identifier, such as the CLI Name. This field displays on the summary and expanded views by default.
Equipment	The name of the resource, such as ISDN card, NIC, and so on. This field displays on the summary and expanded views by default.

Column	Description
Card Description	A description of the resource, such as the card part number. This field displays on the summary and expanded views by default.
Card Type	The type associated with this resource, such as slot, ISDN card, NIC, Other, and so on. This field displays on the summary and expanded views by default.
Operational State	An indicator that shows whether the resource is: • **Active** shows that the card is operable and currently in use with operating capacity available to support further services. • **Busy** shows that the card is currently in use with no operating capacity to spare. • **Disabled** shows that the card is not operable because of a fault or unavailable resources. • **Enabled** shows that the card is operational and available for use. • **Not Determined** show that the state is not determined. This field displays on the summary and expanded views by default.
Date Created	The date this resource entered the database. This field displays on the summary and expanded views by default.
Active Ports	The number of active ports related to a resource. By default, a port is considered active if the administrative state is up. You can modify this functionality to use the port's operational state to determine whether a port is active or inactive by adding the following property to your installed.properties file, saving the file, and then restarting the application server: `com.dorado.redcell.inventory.ActivePortAttribute=OW_OperationalState` This attribute only updates when the device re-syncs.
Administrative State	The interface's current administrative state, such as down, testing, unknown, or up.
Alarm Severity	The highest severity of any existing alarms against this resource.
Alarm Suppression Description	The description provided for an alarm suppression configuration.
Alarm Suppression Mode	A boolean setting (on/off). If Ad Hoc suppression is listed, the device does not receive alarms.
CLI Name	The command line resource name.
Container Index	The container index number.
Creator	The name of the person or process (such as, a discovery rule or device driver) that created this interface.
Domain ID	The identifier for the resource domain.
Firmware Version	The resource's firmware version.
Foreign ID	An optional identifier for the customer's organization.
Hardware Version	The card's hardware version.
Card Icon	The icon that represents the resource.

Column	Description
Inactive Ports	The number of inactive ports related to a resource. By default, a port is considered inactive if the administrative state is **not** up. You can modify this functionality to use the port's operational state to determine whether a port is active or inactive by adding the following property to your installed.properties file, saving the file, and then restarting the application server: `com.dorado.redcell.inventory.ActivePortAttribute=OW_OperationalState` This attribute only updates when the device re-syncs.
Install Date	The time and date the resource was installed.
Model	The number that identifies the resource model.
Notes	A text field for information about the resource.
Physical Index	The given index associated to the resource. This is useful when a vital device component, such as a power supply or fan has sensors attached.
Rack Number	The number that identifies on which rack the component (card, port, or interface) is installed. This is useful when you have larger chassis that have internal racks.
Serial Number	The resource's serial number.
Slot Number	An attribute set by the OMNM product.
Software Version	The resource's software version.
Subslot Number	The number that identifies which slot on the card that the service module is installed. Cards have the potential of supporting child modules, configurable service modules installed on the card.
Total Ports	The total number of ports related to a resource. This attribute only updates when the device re-syncs.

Pop-Up Menu

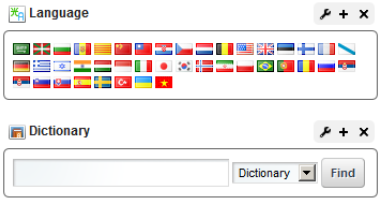
The Cards pop-up menu provides access to the following options. Right-click a row to access these options.

Menu Option	Description
Edit	Opens the Editing *cardName* window, where you view or modify the general details and card properties.
Details (Click+Shift)	Shows the general, alarms, and event history details for the selected card.
Edit Custom Attributes	Opens the Custom Attribute Editor window, where you add or modify attribute definitions.
Share with User	Opens the Share with User window where you select the colleague you want to share this asset with and then type your message.

The Language portlet displays flags indicating languages available for many non-OMNM portlets and menus. By default, this portlet does not reside on any OMNM pages. Click a flag to change menus and titles to the related language.

It is listed under Portal Applications > Tools on the applications list.

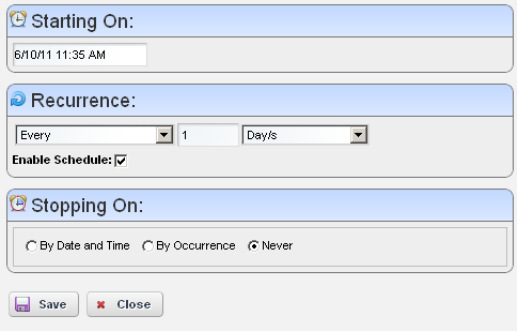
Note that the Dictionary is a seperate portlet. Follow these similar steps to add the Dictionary portlet.



Schedule

Use the Schedule options to schedule an action. These options display in either a window's panel or a window of its own depending on how you accessed them. whether you selected the Schedule pop-up menu option from a portlet, clicked the .

Access the Schedule options from a portlet that ordinarily executes schedules using the Schedule pop-up menu option, clicking Schedule button from a window, or selecting the Schedule tab from a window. For example, right-click a discovery profile and then select Schedule from the Discovery Profiles Portlet. Alternatively, right-click in the Schedules or Configuration Management Schedules portlets, select New > *actionType* > Schedule.



Once you save the schedule, the action (for example Discovery Profile) also appears in the Configuration Management Schedule portlet as a scheduled item.

If you have the OpenManage Network Manager Change Management/Proscan capabilities installed, use Schedules to initiate the Change Determination process. See Change Determination Process on page 344. It is disabled by default.

The following descriptions provide more informatioin about the Schedule fields and options.

Field/Option	Description
Starting On	Sets the date and time to execute the selected action.
Recurrence	Specifies how often to execute the selection action. Select one of the following recurrence types: • **Every**, the number, and unit of measure (Minutes, Hours, Days, Weekdays, Weekend Days, Weeks, Months, Years) • **Increment** (by minutes) and then specify the number of minutes • **Only at Startup** • **Only Once**
Enable Schedule	Activates the schedule when selected.
Stopping On	Sets whether to stop by date and time, occurrence, or never. If you select By Date and Time, the information displays in the *m/d/yy h:mm a* format. If you specify By Occurrence, specify the number of occurrences.

Manage Page

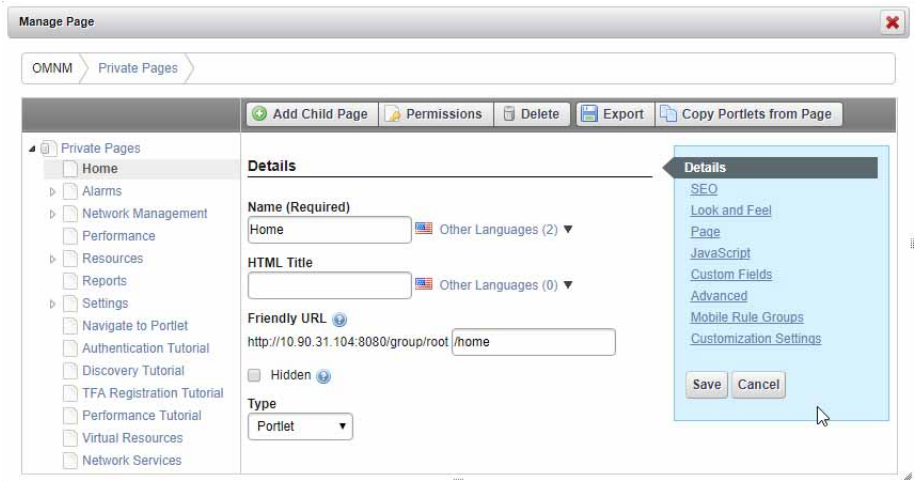
Use the Manage Page window to to configure, add, or delete pages and to manage their appearance and permissions. You must refresh any altered page before edits take effect. Use the Copy Portlets from Page *option* to duplicate another page's portlets on the selected page.

Alter the following portal components:

- Page permissions, appearance, order (using drag-and-drop), and so on
- Child page creation
- Page configuration import/export
- Page layout column configuration

  This option is not available if you have an expanded portlet open because the focus is not in the context of a page.

Access this window by selecting the Manage > Page or Manage > Page Layout menu option.



Show Versions

Use the Show Versions portlet to see which products and versions are installed. This portlet has the following panels:

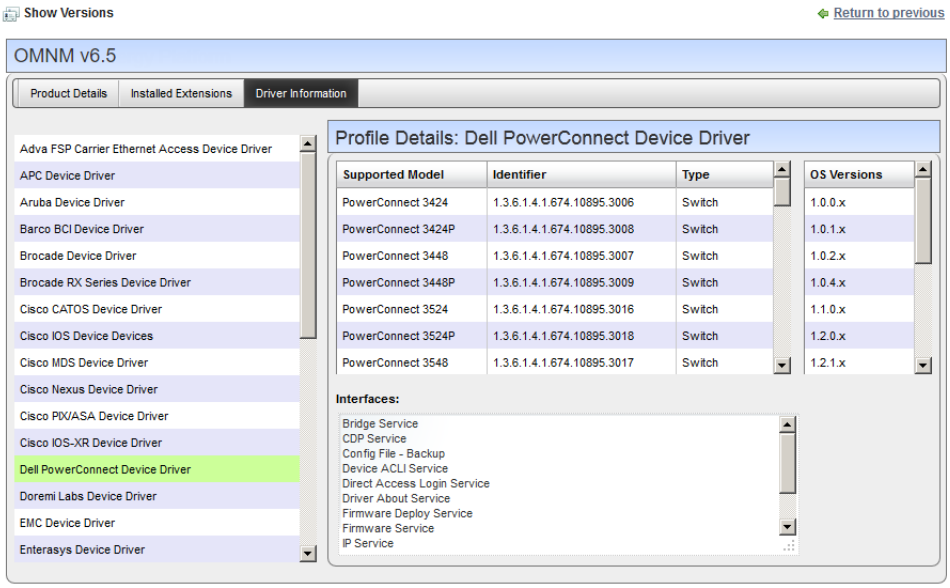
- Product Details displays the installed package and modules, as well as their version numbers.
- Installed Extensions displays any installed presentation layer enhancements.
- Driver Information displays individual drivers (see Base Driver on page 66).

  The Profile Details outlines the supported device models, identifiers (OIDs), types and interfaces, and the OS Versions supported by the driver (although not device-by-device). This information is important when you need technical support.

NOTICE

You can also produce an HTML version of this information from a command line. Run `drvrpt` (drvrpt.cmd in Windows) from the \owareapps\ddbase\bin directory. The drvrpt command saves the HTML version in the *installRoot*\reports\drivers directory.

Access this portlet by selecting the *Manage* > *Show Versions* menu option.

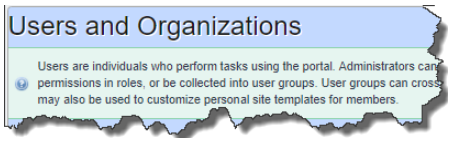


Control Panel

Use the Control panel to configure access to the OpenManage Network Manager system. You must be signed in as a user with administrative permissions. (The default *admin* user has such permissions.) The *Go to* > *Control Panel* menu item opens a screen with the following tabs of interest:

- Administrator
- [Domains]
- Portal > Users and Organizations
- Public/Private Page Behavior
- Portal > Roles
- Portal > Portal Settings
- Portal > [Other]
- Redcell > Permission Manager
- Redcell > Database Aging Policies (DAP)
- Redcell > Data Configuration
- Redcell > Mediation
- Redcell > Filter Management
- Redcell > Application Settings
- Server Administration

Each screen begins with its description. Click the question mark button to hide or show this description. Tool tips appear when you hover the cursor over fields, or click the question mark button.



Users without Administrator permissions may not see all of the features described in this guide.

See Control Panel on page 673 for the Control Panel capabilities.

Search Indexes

Sometimes OpenManage Network Manager may display Control Panel objects like users, roles, and organizations inaccurately. This occurs because search Indexes need to be re-indexed every so often, especially when changes to roles, users and organizations are frequent.

To re-index go to Control Panel > Server Administration and then click on the *Reindex all search indexes*. This takes little time.

Administrator

Administrator

To configure information for your login, look for the bar titled with your account login's name. It has the following lines beneath it:

My Account—This configures your information as a user, including your e-mail address, password, and so on.

Contacts Center—This configures contacts, in other words, people within your system that you are following. This is *not* the same as customer contacts as in the Contacts portlet (see Contacts on page 647).

Click the *Find People* link to see a list of potential contacts within your system. You must click *Action* > *Follow* to see them listed in the *Contacts Home*. Use the *Action* button to explore other possibilities.

The contact has to approve you in their requests. To *Follow* means you want to receive the followed person's activity stream, blog postings, and so on. *Friend*ing means your friends can see your activity and you can see theirs. They have to accept any *Friend* request.

NOTICE

You can export vCards for all contacts in the system to use with other software that uses contacts. For example: e-mail clients.

[Domains]

[Domains]

A default domain name (OMNM) appears in *Control Panel*. *Global* and *Administrator's Personal Site*, or *[Multitenant Site Names]* site configurations may appear as additional items to configure when you expand the domains list. The *Global* option is unrelated to Dell EMC OpenManage Network Manager functionality. Refer to the *Installation Guide* or online help for more about Multitenancy, also referred to as MSP (Multitenant Service Provider) capabilities.

NOTICE

See whether Multitenancy is installed from the Manage > Show Versions > Installed Extensions list. It shows as the Synergy MSP Extension.

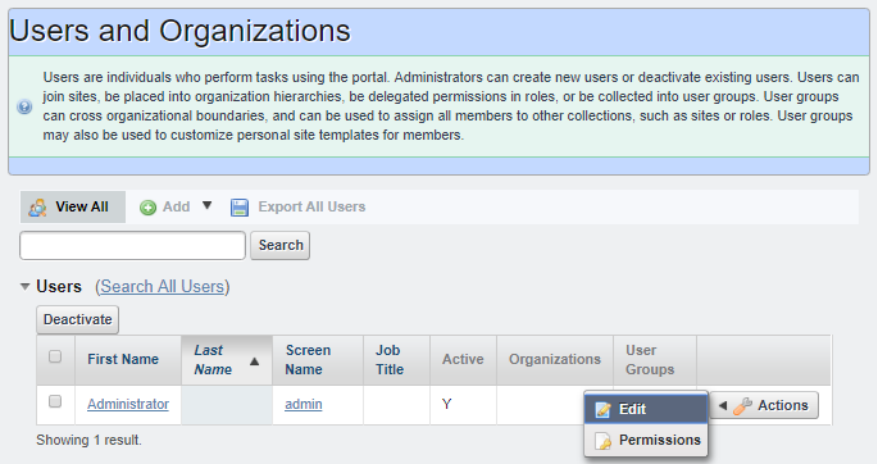
The domain options configure the site settings and the portal's overall look and feel, reference information, and so on. See the tooltips for more complete descriptions. This also configures pages, documents, calendars, blogs, wikis, polls and so on.

Social Activity lets you alter measurements for user participation in organizations. Equity values determine the reward value of an action; equity lifespans determine when to age the reward of action.

Portal > Users and Organizations

In these screens you can create Users you later assign to Roles and Locations with the appropriate permissions (Roles for operators, administrators, and so on). The limit for User Names is 70 characters. Define the default password policy in the Control Panel under Portal > Password Policies.

Users perform tasks using the portal. Administrators can create new users or deactivate existing users. You can organize users in a hierarchy of organizations and delegate administrative rights.



After creating them, add Users to roles which configure their permissions for access and action with the *Actions* menu to the right of a listed user, or during user creation.

NOTICE

Best practice is to spend some time designing your system's security before creating users, organizations and roles.

NOTE:

By default, every new user has the *Power User* and *User* roles. To assign a new user to specific permissions only, remove all rights on these roles, or confine their permissions to those that are universal first. You can remove users from *Power User*, but not from *User*.

When signed in, you can edit your user information by clicking the link with your username in the top right corner of the screen.

User/Power User Roles

This role's description is *Portal Role: Portal users with view access*. To turn off most permissions from the User Role, go to Redcell > Permission manager and edit the User role. The *Advanced* button opens a screen where you can select/de-select permissions in larger groups. Power User is *Portal users with extended privileges*, and Administrator is *Portal users with system privileges*.

Default User Roles — Power User

To make new users *not* assigned as Power Users by default, go to the Portal > Portal Settings > Users > Default Associations Tab and remove the roles you do not want assigned by default. Notice that you can assign/unassign to existing users in this tab too. The role User appears in this default list, but removal does not have an impact. OpenManage Network Manager automatically assigns all users to the User role, so you must modify it as a universal minimum of permissions.

Multitenancy and Roles

For a new user that is part of Customer Turnup, OpenManage Network Manager always assigns the Power User role, regardless of defaults, since it is a Site Contact.

Public/Private Page Behavior

Despite the small *Public/Private* label next to the My Private/My Public pages listed in the *Go To* menu, both types of pages appear only for the user(s) who created them. Page Standard settings are *Max Items*, *Default Filter*, *Max Items per Page*, and *Column Configuration*. These persist for Admin users on the RCSynergy pages, or for users who have the portlet on their Public or Private pages (which makes them the owner of that instance). Without OpenManage Network Manager portlets, URLs for pages labeled public are accessible even to users who do not log in.

Some portlets provide extra settings—for example Alarms portlet's charting options, or the *Top N* portlets number of Top Items. These persist too.

NOTICE

Max Items, *Max Items Per Page* and *Columns* persist for both the summary and maximized portlets independently. For example: If Max Items is 50 in minimized mode it does not affect the Max Items in the Maximized window state. This lets you configure modes independently.

OpenManage Network Manager remembers the default sort column and order per user, whether the user has Admin rights or not. The Sort Column/Order (Descending/Ascending) is also shared between both summary and maximized portlets. A sort on IP Address in Resources persists if you expand the summary portlet to maximized mode.

The *My Public* and *My Private* pages do not appear in sites that have Multitenancy enabled unless you access them through Portal > Sites in the Control Panel. These pages are unrelated to user-specific pages in non-Multitenant installations. They refer to the site, not the user. Refer to the *Installation Guide* for more information about Multitenancy.

In any case, the administrative user can re-arrange pages and portlets in a way that persists. Non-administrative users typically cannot do this.

Portal > Roles

Roles determine the applications permissions available to users assigned them; manage them in the *Portal > Roles* screen. Notice that these permissions are for the web portal's open source capabilities. You can click the *Actions* button to the right of listed Roles to change a role's portal capabilities. To configure OpenManage Network Manager's functional permissions, over and above portal capabilities, use the editor described in Redcell > Permission Manager on page 678.

Click *Add* to create a *Regular Role*, *Site Role*, or *Organizational Role*. A *Regular Role* assigns its permissions to its members. A *Site* or *Organizational Role* assigns portal permissions to a site or organization to which you can assign users. Other than for *Regular Role*, however, only web portal

permissions (not OpenManage Network Manager permissions) are available for *Site Roles* and *Organizational Roles*. Only *Regular Roles* restrict a user's OpenManage Network Manager abilities.

Click the *Action* button to the right of a role to *Edit*, view or alter *Permissions*, *Assign Members* (this last works to see and assign users). You can also assign role members in the Portal > Users and Organizations user editor.

NOTE:

Owner Roles do not have an *Action* button. Owner implies something you have added or created and so actions do not apply.

Notice also that when you *Assign Members*, a screen appears with tabs where you can assign *Users*, *Sites*, *Organizations* and *User Roles*. Typical best practice is to assign users to one of these collective designations, then assign the collection to a Role.

Notice also that you can view both *Current* and *Available* members with those sub-tabs. You can even *Search* for members.

Click *Back* (in the upper right corner) or the *View All* tab to return to the screen listing roles and their *Action* buttons.

Portal > Password Policies

This panel lets you configure password policies for your installation. It includes options that configure whether and when change to passwords must occur, syntax checking, history, expiration, and lockout policies for failed logins.

NOTE:

For users of Multitenant sites, logins require the prepended site prefix. For example, an admin user in customer site with prefix BP, logs in as BP-admin.

You can also generate a User Login Report/Last 30 Days to view the history of logins.

Portal > Portal Settings

The *Settings* screens are where users who are administrators can configure the most basic global settings for OpenManage Network Manager, including names, authentication, default user associations, and mail host names. These include the following:

- Users — Among other things *Default User Associations* configures Site and Role defaults for users. Remember, you can remove the Power User default here, but removing the User role does not work. You have to change permissions for User because every user gets that Role.
- Mail Host Name(s) — These are for user account notifications, not mail hosts for OpenManage Network Manager event-based notifications configured in Event Processing Rules, for example (see Automation and Event Processing Rules on page 512). Configure such notifications as described in SMTP Configuration on page 626.
- Email notifications, who sends them, what the contents are for account creation notices, or password change/reset notices.
- Identification, including address, phone, email and web sites.
- The default landing page, and display settings like the site logo.

- Google Apps login/password.

CAUTION:
Checking *Allow Strangers to create accounts* may produce a defective login screen. Do not do it.

Portal > [Other]

Some of the remaining portal items permit the following:

Sites—Configure sites. Sites are a set of pages that display content and provide access to specific applications. Sites can have members, which are given exclusive access to specific pages or content. Refer to the *Installation Guide* (or online help) for a more in-depth explanation of Multitenancy and the real power of sites.

Site Template—Configures pages and web content for organizations. Refer to the *Installation Guide* (or online help) for a more in-depth explanation of Multitenancy and the real power of sites.

Page Template—Configures a page and portlets, as well as permissions. Refer to the *Installation Guide* (or online help) for a more in-depth explanation of Multitenancy and the use of Page Templates.

Password Policy—Configure the security policies you want, including user lockout and password expiration, and assign them to users.

Custom Fields—Lets you configure custom fields for Blog entries, Bookmarks or Bookmark Folders, Calendar Events, and so on.

Monitoring—Lets you see details like accessed URLs, number of hits, and so on, for live sessions on the portal. Click a session to see its details. This is usually turned off in production for performance reasons.

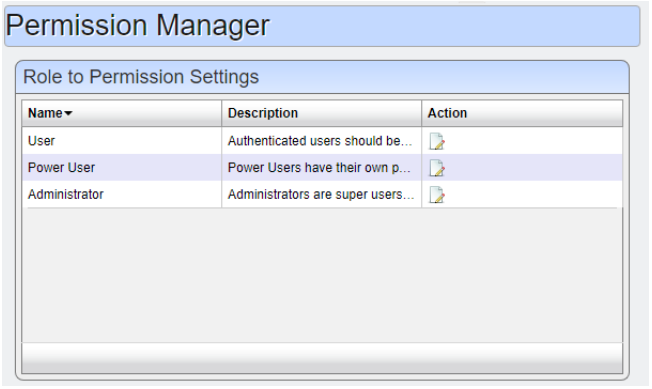
Plugins Configuration—Configure access to portlets and features like themes, layouts and so on. By default, only administrators can add portlets/plugins to their pages.

Redcell > Permission Manager

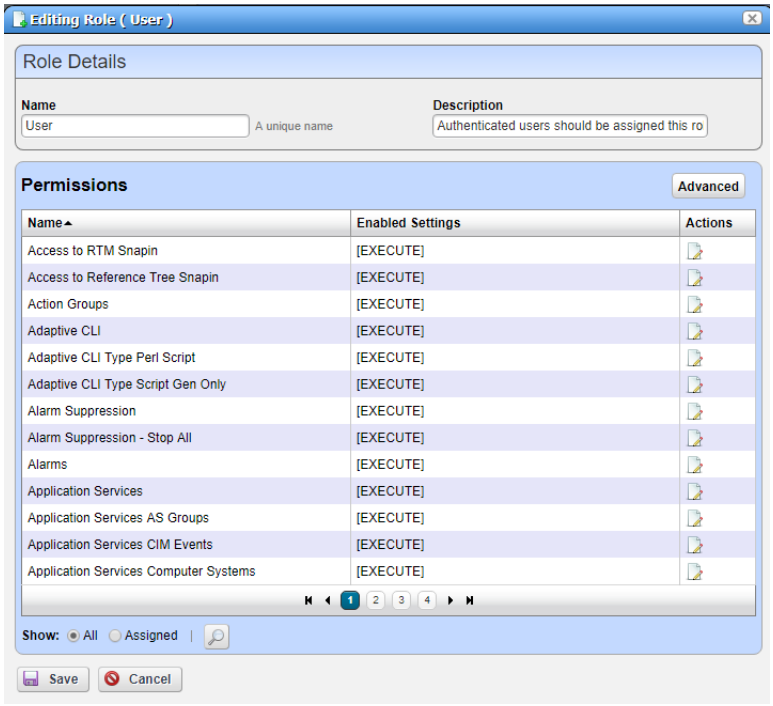
Manage Permissions in these panels to manage user access to different OpenManage Network Manager features. These are configured as part of Roles, which aggregate users regardless of community affiliation. Create Roles with Portal > Roles.

Notice that, by default, *User*, *Power User* and *Administrator* roles exist and have OpenManage Network Manager permissions. Also, by default, the application assigns *User* and *Power User* roles' permissions to any new users you create. Since OpenManage Network Manager logically ANDs all permissions, this may mean you want to alter the defaults that come with these roles too. You can remove the *Power User* default in the Portal > Portal Settings > User > Default User Associations panel, but removing the *User* role from these default assignments is ineffective, so take care to configure *User* to reflect your system's requirements.

The *Users* editor screen accessible from the *Action* menu for users listed in Portal > Users and Organizations lets you manage groups to which Users are assigned.

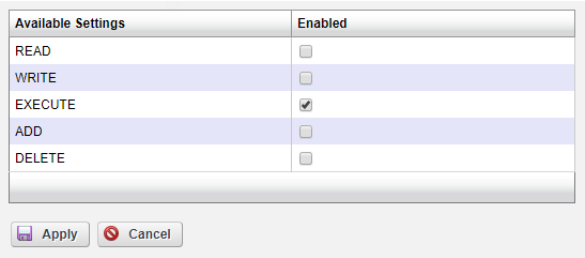


Click the Actions Edit button to see and configure its permissions.



Notice that you have the option to view *Assigned* or *All* permissionsor search for the permission you want to locate.

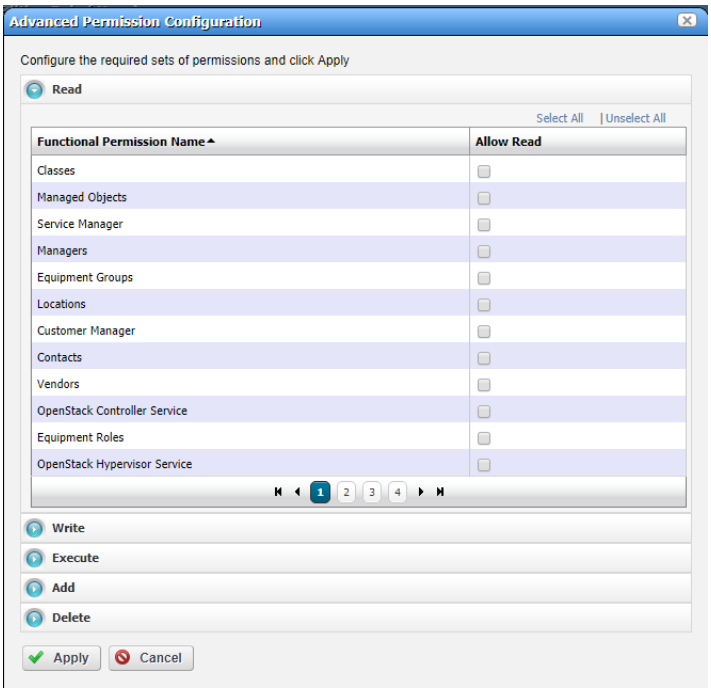
Click Actions *Edit* button to modify the type of permissions available.



The following describes the actions of the permissions, when checked:

Action	Default Behavior
read	Enables *Details*, *Visualize* and *View as PDF*
write	Enables the *Edit*, *Save*, and *Import/Export*.
execute	Lets you see the view altogether, launch from a portlet and query for elements. Alternatively this action can control a specific application function, (typically described by the permission name) like provisioning a policy.
add	Enables the *New* menu item, and *Save*. If you do not check this action, then the *New* menu item does not appear.
delete	Enables the *Delete* menu item.

The *Advanced* button lets you configure each functional permissions by type. For example, expand the Read list to specify READ permissions to all or selected functions.



When you hover the cursor over a functional permission, tooltips provide a description.

NOTICE

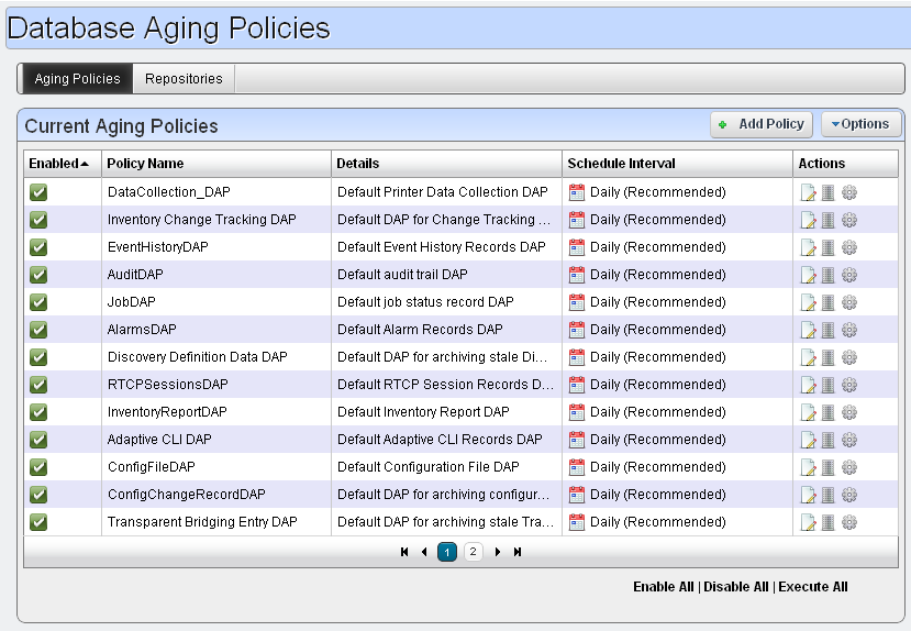
If you upgrade your installation and new permissions are available, edit the Administrator Role, and notice an enabled *Add* button indicates new permissions are available. Because of an upgrade, for example, the Configuration Files portlet might not be visible. By default, upgrades turn off any new permissions, so if you want them enabled, particularly for Administrators, click *Add* and enable them for the Roles for which you want them enabled.

The portlet settings button (wrench) through which you edit portlet settings, is only accessible if you have the "Change Portlet Settings" permission. On upgrade, no users this permission. This is by design, because the intent is for the system administrator to consider which users (more specifically, which user roles) should change portlet settings and which users should not have access to this feature.

Redcell > Database Aging Policies (DAP)

Database Aging Policies prevent the OpenManage Network Manager database from filling up by filling up by deleting old records. You can also save designated contents to an archive file on a specified cycle. Database Aging Policies configure which contents to archive, the archive location, and the configuration of that archive file.

To view and manage such policies, right click an item with them (for example, an alarm), or click *Manage* > *Control Panel*, and under *Redcell* click *Database Aging Policies*.



Policies appear in the *Aging Policies* tab of this screen, with columns that indicate whether the policy is *Enabled*, the *Policy Name*, *Details* (description), *Scheduled Intervals* and icons triggering three *Actions* (*Edit*, *Delete* and *Execute*). Notice that the bottom right corner of this page also lets you *Enable/Disable/Execute All* policies listed.

Redcell > Data Configuration

This panel configures custom attributes for OpenManage Network Manager. Click the *Edit* button next to the *Entity Type* (Managed Equipment, Port, Contact, Vendor, or Location) for which you want to create custom attributes. This opens an editor listing the available custom attributes for the entity type. Editing Custom Attributes on page 88 describes right-clicking to access this directly from the portlet menu, and the details of how to edit custom attributes.

NOTE:

The custom fields configured here are for OpenManage Network Manager. only. The Custom Fields editor in the *Portal* portion of Control Panel manages custom fields for the rest of the portal.

Redcell > Audit Trail Definitions

This screen, accessible from Go to > Control Panel lets you manage audit trail definitions in Redcell. Audit trail entries are based on these definitions. Clicking the Edit icon to the right of a listed filter opens the editor. From this screen you can control the behavior of audit trail entries based on each respective definition.

The following fields are available for configuration:

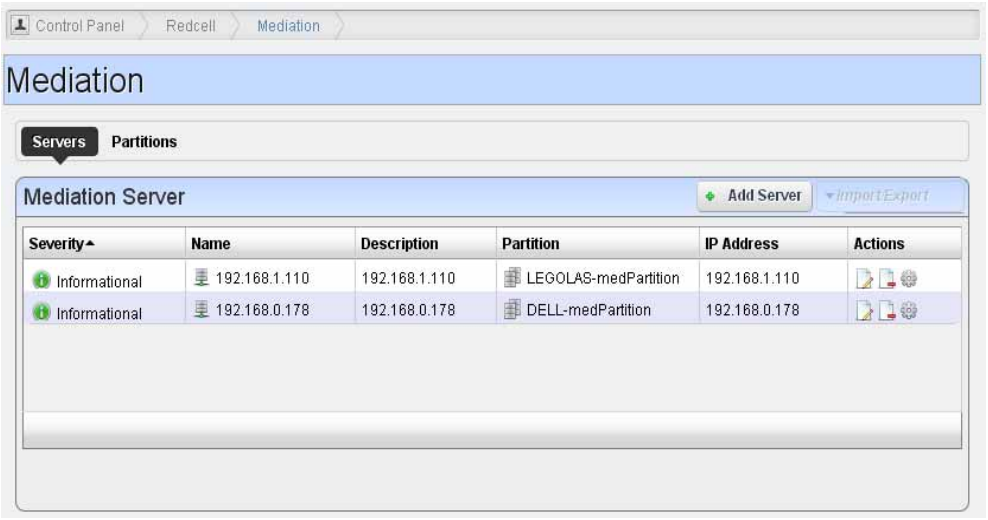
Severity Level - Users viewing the audit trail must have at least this level of security in order to view this type of audit trail. 0 is the most restrictive, so if a definition has a security level of 0 then only users with the highest level of security can see this type of audit trail.

Disabled - Controls whether or not this type of audit trail is saved to the database. If disabled is checked, then audit trail entries of this type are not saved.

Emit Event - Controls whether or not to emit an event when this type of audit trail is created. This can be useful, for example, if you want to forward audit log entries to a northbound system. To do this, simply check Emit Event for the type of audit trails that you want to forward and then create an Event Processing Rule to forward northbound all events of type redcellAuditTrailEntry. Note that the default behavior for the event definition redcellAuditTrailEntry is reject, meaning that these events will not be saved to the event history, but they can still nonetheless trigger the execution of event processing rules.

Redcell > Mediation

This panel monitors mediation servers in your system, appearing only when such servers exist. Mediation servers appear listed in the *Servers* tab of this manager if mediation servers are connected to application servers.



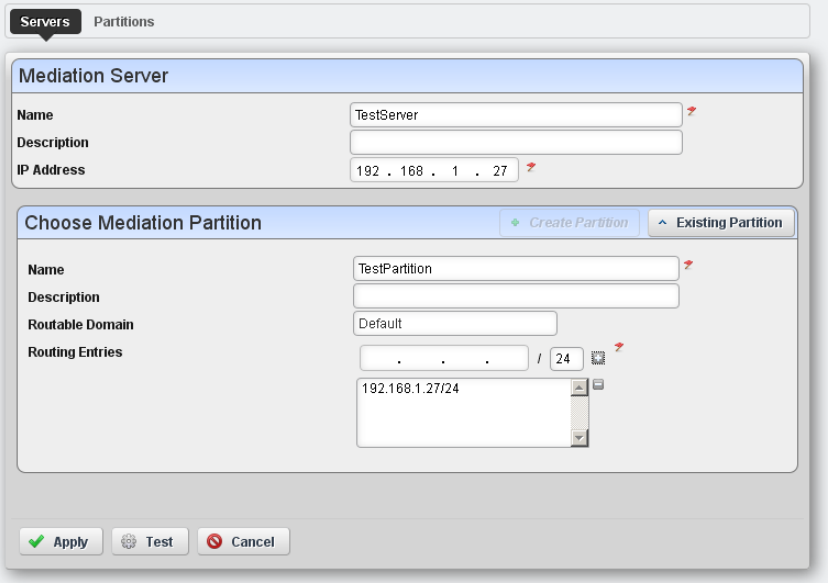
Mediation server, routing entries and partition entries appear automatically when mediation server connects for the first time. You can test connectivity from appserver cluster and medserver/partition.

You can export or import both server and partition configurations. Use the button on the right above the listed servers or partitions to do this. Importing Partitions/MedServers overwrites those in the database with the same names. Exporting a partition exports contained medservers too. Importing a partition looks for overlapping routing entries and saves the partition with only its unique entries. If no entries are unique, the partition is not saved.

NOTE:

This panel does not appear if you install OpenManage Network Manager in stand-alone mode, without a separate mediation server. To make it appear, add `medserver.support=true` to `portal-ext.properties` file in `\oware\synergy\tomcat-7.0.26\webapps\ROOT\WEB-INF\classes`. Remember, best practice is to override properties as described in Overriding Properties on page 71.

In addition to automatically detecting mediation servers, you can click *Add Server* to configure additional mediation servers.



When creating a new server, enter a *Name*, *Description* and *IP Address*. You can also *Create Partition* (or select from *Existing Partitions*), choosing a *Name*, *Description*, *Routable Domain*, and *Routing Entries* (click the '+' to add your entries to the list).

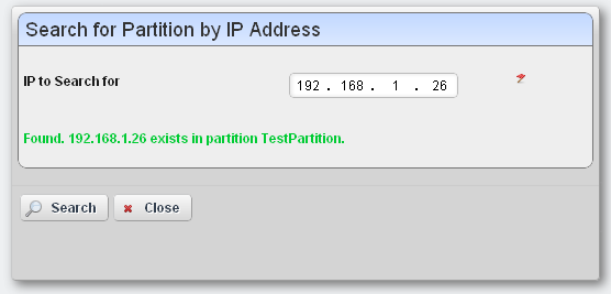
The *Test* button scanning the ports in the proposed application server/mediation server link, validating the installed versions of OpenManage Network Manager in both locations are the same, and validating the connection between application server and mediation server. A window opens similar to the *Audit Trail/Jobs Status* on page 689 that tracks testing progress.

The *Partitions* tab of the Mediation monitor displays already-configured partitions, and lets *Add Partition*, or lets you edit them with an *Edit this entry* icon. The editor screen is like the one that adds new partitions, where you enter a name, description and routable domain CIDR IP addresses.

Test listed partitions with the gear icon to the right of the partition, or delete it with the *Delete this entry* icon. Notice that you can also *Import/Export* partition descriptions with that button on this screen.

Search for Mediation Server

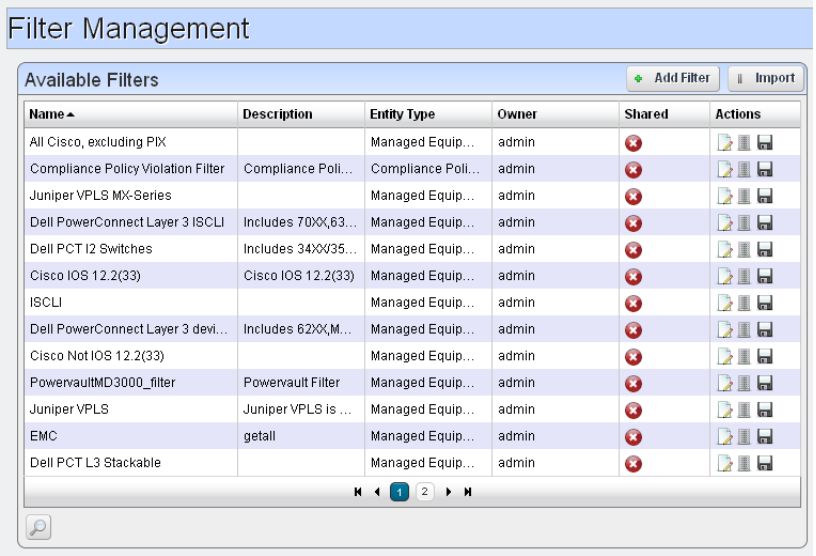
The *Search* button in the *Partitions* tab of the Mediation monitor opens a screen where you can enter an address in *IP to Search for*.



Clicking *Search* locates the mediation partition that services the entered IP address (although it does not determine whether that partition is up and running).

Redcell > Filter Management

This screen, accessible from *Go to* > *Control Panel* lets you manage the filters in OpenManage Network Manager.

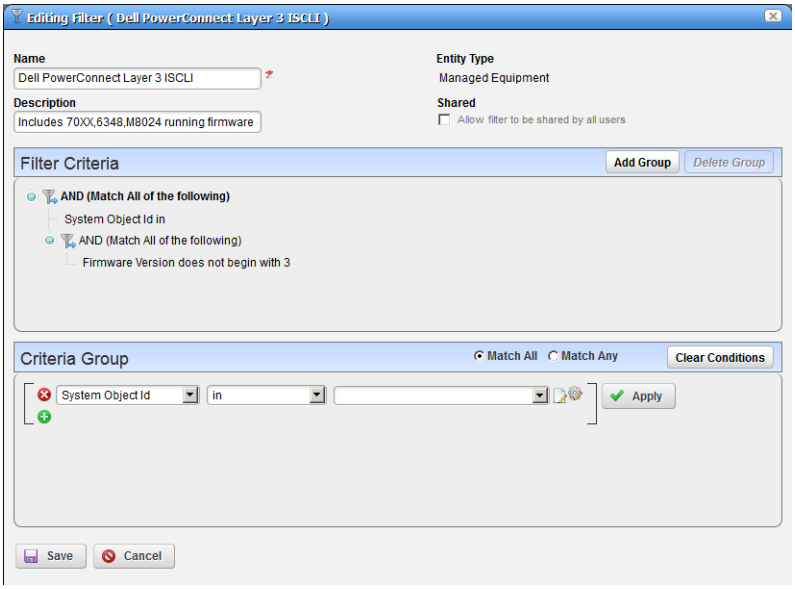


Click the *Delete* icon to the right of a listed filter to remove it from the system. Click the disk icon to export the filter. Clicking the *Import* button at the top of the screen lets you import previously exported filters.

NOTICE

To find a particular filter, click the *Search* (magnifying glass) icon in the lower left corner of this screen.

Clicking the *Edit* icon to the right of a listed filter, or clicking the *Add Filter* button opens the filter editor.



Use this editor to configure filters. Enter a *Name* and *Description*, and use the green plus (+) to select an entity type from a subsequent screen. Checking *Shared* makes the filter available for all users, not just your user. You can add groups of filter criteria (click *Add Group*) that logical AND (*Match All*) or OR (*Match Any*) with each other. Click *Clear Conditions* to remove criteria. Configure the filter in the *Criteria Group* panel as described in the How to: Defining Advanced Filters on page 86. Delete filters with the *Delete this entry* icon next to the edit icon.

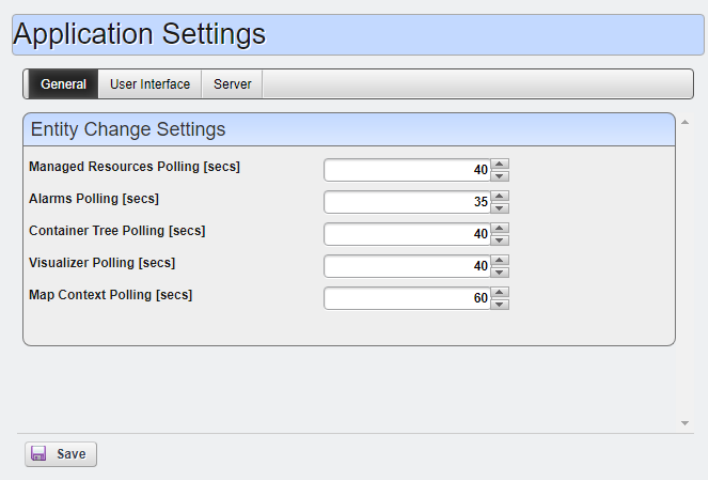
Redcell > Application Settings

This screen has several panels in the following tabs:

- General > Entity Change Settings
- User Interface > Map Provider
- User Interface > Job Viewer
- User Interface > Performance Chart Settings
- User Interface > Revert to Factory Defaults (self-explanatory)
- Server

General > Entity Change Settings

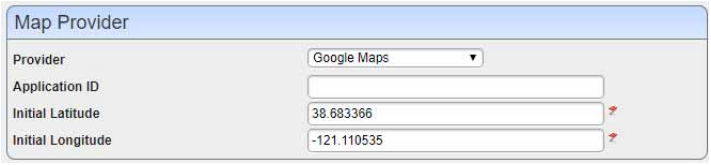
This panel lets you override polling/refreshing for the minimized Managed Resources, Alarms, Container Tree, Visualizer and Map Context portlets. By default, these portlets poll at 40, 35, 40, 40, and 60 seconds, respectively, for changes in the data and automatically refresh. Polling times are configurable.The valid range is 10 seconds -> 3600 (1 hour) for the minimized Alarms porlet, 20 seconds -> 3600 seconds for the others.



User Interface > Map Provider

The *Map Provider* panel lets you set whether OpenManage Network Manager uses Google or Nokia maps by default, and sets the Initial Latitude and Longitude. Check *Use Secure API* if you want to load map APIs in secure SSL mode. Some browsers block non-secure external APIs if they are viewing a secure page, so use this if you view OpenManage Network Manager through an HTTPS connection.

Follow the directions in Setting Up Google Maps on page 145 to set the application to use those maps.



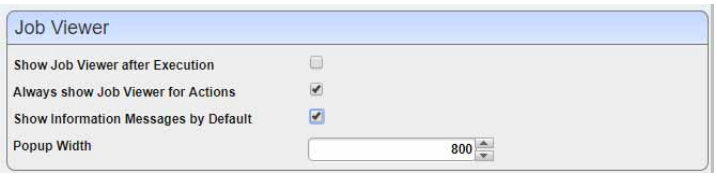
User Interface > Job Viewer

The *Job Viewer* panel lets you select the following options and set the popup width:

Show Job Viewer—Checking this displays the job viewer after Execution (most cases). Leaving it unchecked does not display it, although you can still view jobs with *My Alerts* in the lower left portion of the screen.

Always show Job Viewer for Actions—When checked, this displays the job viewer for execution of Actions or Action Groups.

Show Information Messages by Default—When checked, shows informational message nodes by default.



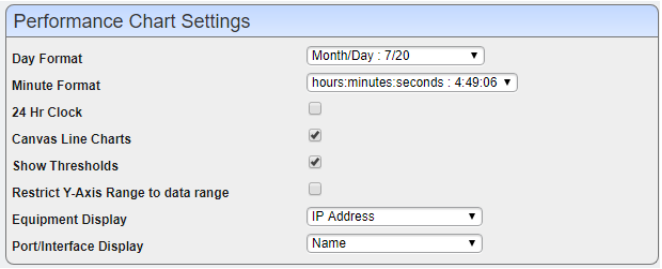
User Interface > Performance Chart Settings

This panel displays options for the performance dashboard and traffic charts. Day and Minute Formats depend on the locale settings in the operating system running OpenManage Network Manager. Select them in the pick lists that appear in this panel. The 24 Hr Clock setting makes the charts show times in 24-hour format.

The Canvas Line Charts option controls the type of line charts that are used. Earlier versions of Redcell used a Scalable Vector Graphics type line chart. Redcell now supports a Canvas based line chart which can display many more points. If you prefer to use the old style SVG line charts you can uncheck this box.

The Restrict Y-Axis Range to data range option causes the Y-axis range to be based on the range of data being graphed. If this is not checked the range will be based on the max and min values associated with the attribute definitions. For example most % values will have a range of 0 to 100.

The Equipment Display setting controls how equipment labels are shown in the performance dashboards. The default is to display the ip address. You can also have it display the device name. The Port/Interface Display setting lets you select between showing the Port/Interface Name of the Port/Interface description.



Server

This panel lets you override the system defaults for web client time-outs. You must configure this if you want your web client to remain connected to the server for extended periods. The timeout extends automatically with any activity (keystrokes) on the client.



Set the timeout with the following fields:

Override System Defaults—Check this to start overriding the system default time-outs for all users.

Timeout [mins]—Enter the minutes of inactivity before Timeout occurs (5 - 2880 [two days])

Role based Extended Inactivity

If you want to confine extended web client sessions to a particular role, then use these fields to configure that.

User Role—Select the role for which this override works from the pick list.

Timeout [days]—Select the number of days for role-based timeout override, up to 365.

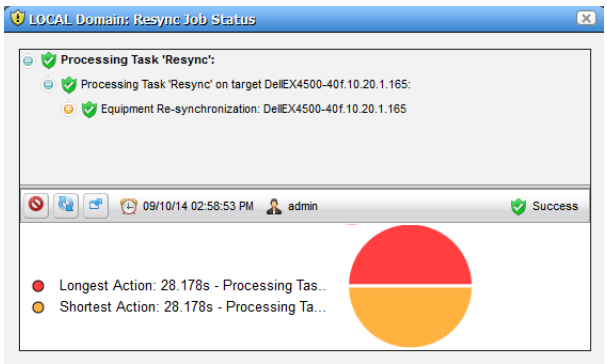
Server Administration

The Server Administration option lets you manage the portal's webserver, and maintain its smoth operation in a variety of ways. Click the Execute buttons to run actions, such as re-indexing the search indexes. These options are visable to administrators only and they contain helpful settings and resource information related to the server..

Access this option by selecting Go to > Control Panel > Server > Server Administration.

Audit Trail/Jobs Status

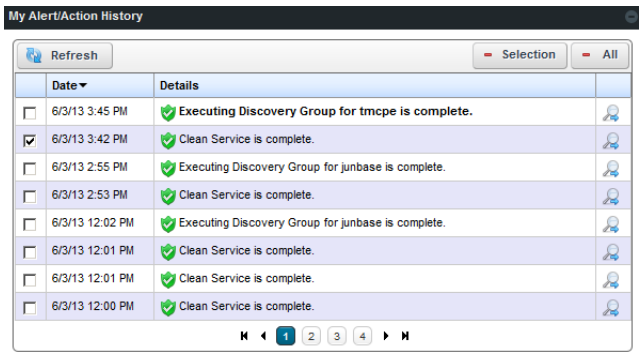
When you execute an action, for example when you resync network resources, an audit trail screen appears with a tree displaying the message traffic between OpenManage Network Manager and the devices the action addresses.



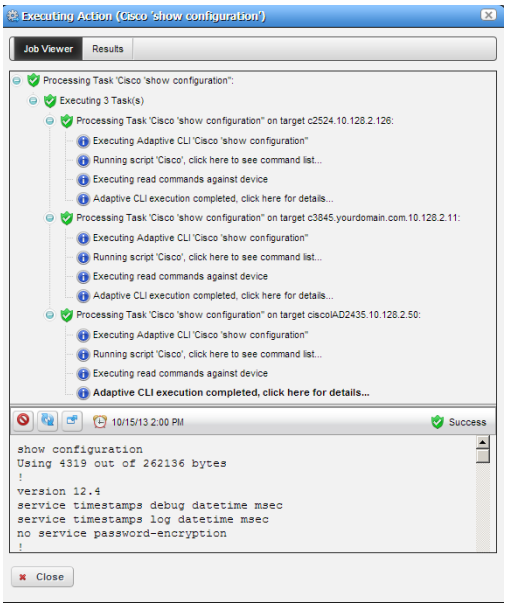
To see the details of any message, click on it, and those details appear in the lowest panel of this screen. If you click on a summary message (not a "leaf" on the tree), a graph appears displaying the duration for its component messages. Hover your cursor over each portion of the graph for more details.

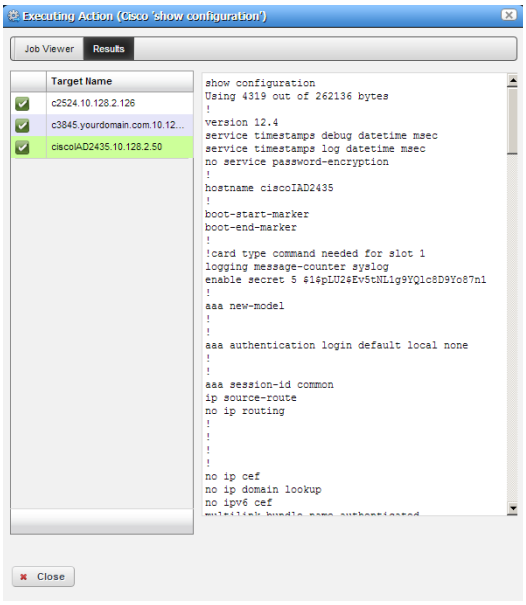
The time for messages and logged in user initiating the action appear on the bar between the upper and lower screen, and an icon summarizing the action appears on its right. Click the second icon from the left to configure the amount of detail displayed in audit messages. Click the first (*Refresh*) icon to re-display messages if you re-configure the type(s) displayed. See View Job on page 632 for illustrations.

To review the audit trail for recently completed processing, open the *My Alerts* tab in the lower left corner of the portal, and click the magnifying glass to the right of the message.



Some audit trails display as many as three tabs for the *Input* (the command variables sent to the device), the *Job Viewer* with the message traffic to the device, and the *Results* of sending the messages to a device. By default, this screen conceals the info-level messages. To see them, click the the Refresh icon to open the message level selector and and select the info circle level of reporting, then click Refresh to see those blue circles. The Results lists devices on the left, and message traffic for a selected device on the right.





Close the audit trail viewer any time, and the action continues in the background. The the audit trail is archived in the portlet described in Scheduling Actions on page 307.

Cancel Option

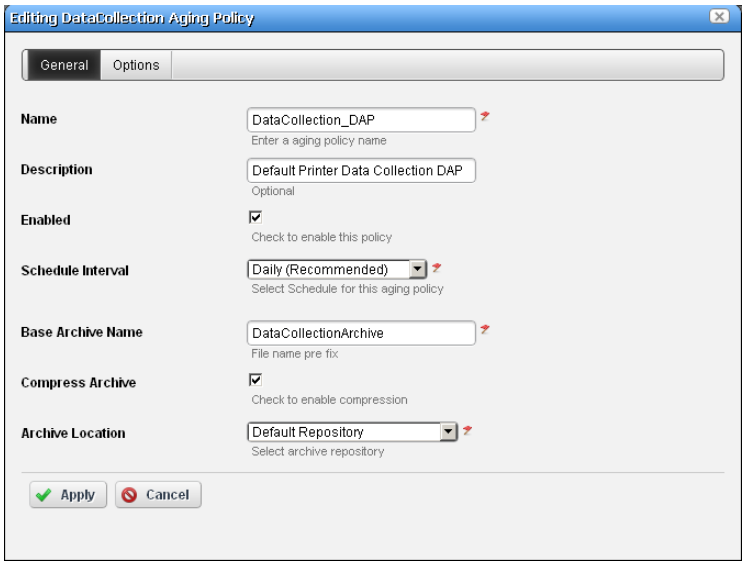
Audit trails/job screens sometimes display a "Cancel" icon. This stops some, but not all jobs in progress. The underlying feature (Discovery, Resync, Backup, and so on) described in the audit trail is responsible for gracefully stopping the execution flow, ensuring that the system and the database is left in a good state; not all features can do this. For performance reasons, it checks for cancellation at appropriate spots in the transaction where it is easy and safe to exit the execution flow. This means that even if the type of job supports cancellation, it may not cancel the current

execution. If you press cancel while in the middle of a multiple-device resync, OpenManage Network Manager does not stop the resync for that device but instead bypasses the resync of subsequent devices.

Cancellation does not roll back work that has already been completed. So if you are executing an Adaptive CLI action against 10 devices and you cancel the job after the third device is configured OpenManage Network Manager does not try to roll back the work that has already occurred against the first three. However, it does stop executing against the remaining seven.

Aging Policies Editor

When you click *Add Policy* in the upper right corner of the Redcell > Database Aging Policies (DAP) screen, first a selector appears where you can click on the kind of policy you want to create, then the editor appears. If you click the *Edit* icon to the right of a listed policy, the Aging Policies Editor appears with that policy's information already filled out, ready to modify.



The *General* screen has the following fields:

Name—An identifier for the policy

Description—A text description of the policy

Enabled—Check to enable the policy.

Schedule Interval—Use the pick list to select an interval. Once you have configured an interval here, you can re-configure it in the Schedule portlet.

Base Archive Name—The prefix for the archived file.

Compress Archive—Check to compress the archive file.

Archive Location—Select from the available Repositories in the pick list.

The contents of the *Options* tab depend on the type of DAP you are configuring. Typically, this tab is where you set the retention thresholds.

DAP SubPolicies

Some Options tabs include sub-policies for individual attribute retention.



Click *Add SubPolicy* or click the *Edit* button to the right of listed policies to access the editor. The fields vary depending on the policy selected.

Editing Tips

Archiving options that appear in the Aging Policies Editor vary, based on type of policy selected. Inventory Change Tracking DAPs ask how long you would like to keep Config reports, Inventory Report DAPs ask how long you would like to keep your Historical Reports based on number of instances, days, and weeks, months or years.

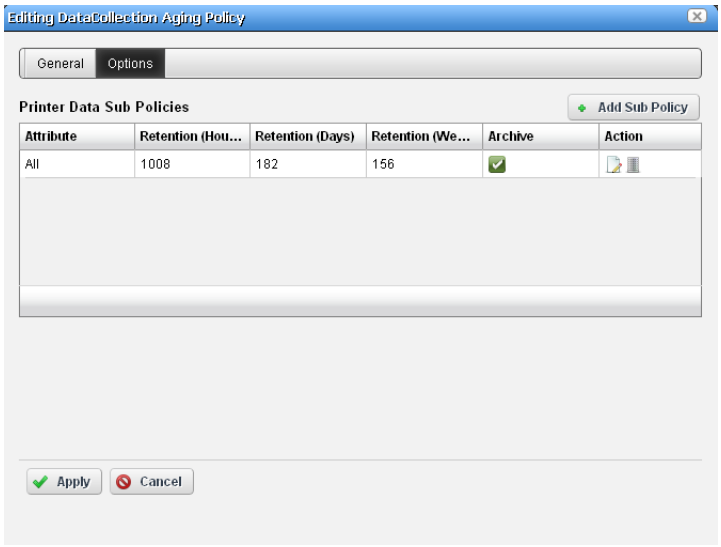
Set these thresholds in the *Options* tab. All DAPs require a Name and a record threshold. Check the *Enabled* checkbox to enable the policy.

DAPs run on a schedule. If the record threshold number is greater than or equal to the configured threshold then the DAP runs at the scheduled time. You may also manually click the gear icon to the right of a listed policy, and execute a DAP at any time to check that threshold figure. In either case, if the threshold is not crossed OpenManage Network Manager creates no archives.

To verify when current DAPs are scheduled to run, open the Schedules portlet, and select the schedule on which it runs. For most DAPs, this is the Daily (recommended) DAP. Right-click to edit it. The Scheduled Aging Policies list should include all DAPs that have selected that schedule.

Aging Policies Options

The *Options* tab in this editor can vary, depending on the type of policy.



Fields can include the following:

Keep [Aged Item] for this many days—The number of days to keep the aged item before archiving it.

Archive [Aged Item]—Check this to activated archiving according to this policy.

Sub-Policies

Some types of Database Aging Policies can have sub-policies that further refine the aging for their type of contents.

These appear listed in the Aging Policies Options tab. Click *Add Sub Policy* to create them. Notice that you can *Edit* or *Delete* listed policies with the icons in the far-right *Action* column in this list.

Such sub-policies can contain the following types of fields:

Component—Select the component for the sub-policy from the pick list.

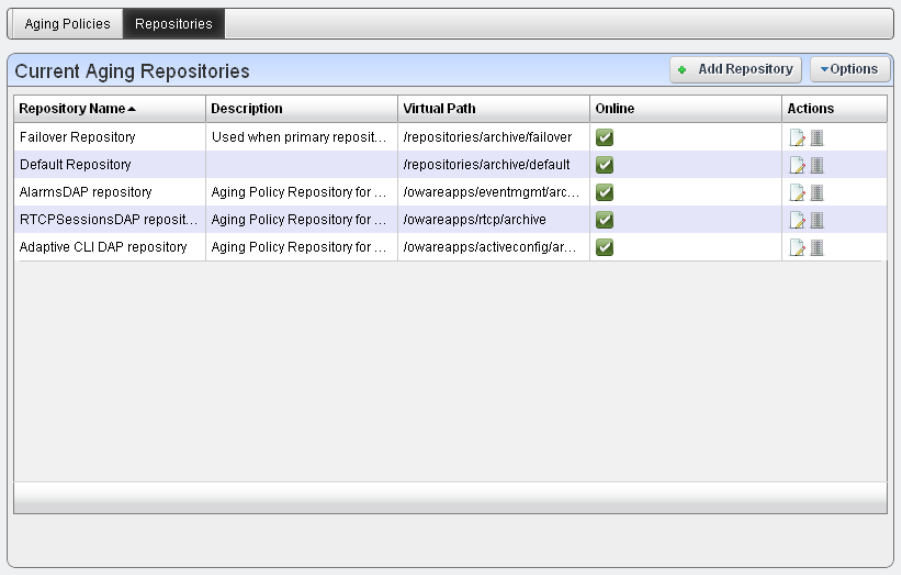
Action Type—This further sub-classifies the *Component*.

Retention (Days)—The number of days to keep the aged item before archiving it.

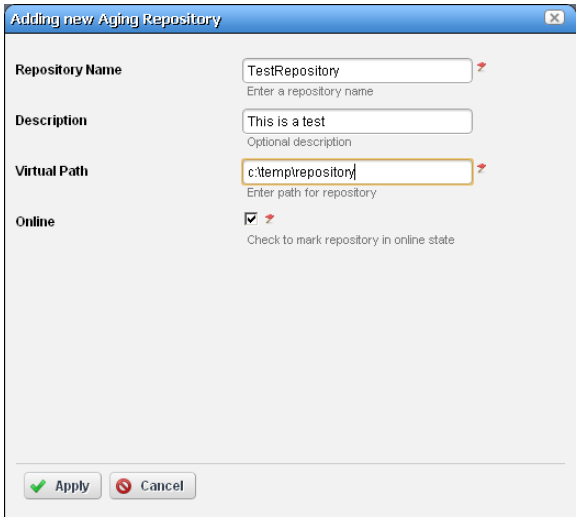
Archive—Check this to activated archiving according to this policy.

Repositories

When you select a repository in the Aging Policies Editor, the available policies come from what is configured in this tab of the editor.



Available repositories appear listed in the initial screen. Like the Aging Policies Editor, you can click *Add Repository* to create a new repository, and *Edit* or *Delete* selected, listed policies with the icons in the *Action* column. Notice the listed policies indicated whether the archiving destination is *Online* with a green icon (this is red, when the destination is offline).



When you *Add Repository* or *Edit* an existing one, the following fields appear in the editor:

Repository Name—An identifier for the archiving destination.

Description—A text comment.

Virtual Path—This is the path relative to the installation root directory. Any user with administrator permissions can specify or change the default archive path here.

Online—Check this to put this repository online.

OpenManage Network Manager automatically writes to any configured failover repository if the primary repository is full or not writable.

NOTICE

To view any archived DAP file, use `dapviewer`. Type `oware` in a command shell, then, after pressing [Enter], type `dapviewer` to use this utility.

B

Ports Used

The following reference material is provided in this section:

Standard Port Assignments – 698
Protocol Flows – 703
Ports and Application To Exclude from Firewall – 708
Installed Third Party Applications – 709
Windows Management Instrumentation Ports – 710

Standard Port Assignments

Initial installation scans the following ports, and reports any conflicts with them:

Database: 3306 or user-configured database host, if using MySQL server.

Application server: 8089, 8162, 8489 [HTTPS], 8082

Web Portal: 8080, 8443 [HTTPS]

SNMP: 161, 162

Syslog: 514

When installation encounters a conflict with any of the above ports, a panel appears displaying a warning and the port[s] in conflict. You can then elect to continue since you can change the application ports after installation. If installation encounters no port conflicts, then no panel appears.

NOTE:

The installation scans TCP ports to detect potential conflicts. It does not scan UDP port conflicts including SNMP Ports 161 and 162. No SNMP or other applications should bind to UDP ports 161 and 162 since such bindings interfere with the application. If this conflict exists, the following error appears (with others):

```
FATAL ERROR - Initializing SNMP Trap Listener
```

You may also configure network ports' availability on firewalls. Sometimes, excluding applications from firewall interference is all that is needed (see Ports and Application To Exclude from Firewall on page 708). If you have remote mediation servers, see Remote Mediation Ports on page 703.

The following are some of the standard port assignments for installed components. These are often configurable, even for "standard" services like FTP or HTTP, with alterations to the files mentioned, so these are the default, typical or expected port numbers rather than guaranteed assignments. Also, see Protocol Flows on page 703 for more about network connections. The JBoss directory number may vary with your package's version; *.* appears rather than actual numbers.

Destination Ports	Service	Files	Notes
3306	Database		... or user-configured database host, if using MySQL server.
8089, 8162, 8489 [HTTPS], 8082	Application server		
8080, 8443 [HTTPS]	Web Portal:		
HTTP/S (Web Client)			
8089[4]	oware.webservices.port	[user.root]\oware\lib\owweb services.properties	appserver. **Note:** this port was 80 in some previous versions.
8489[4, 5, 7]	org.apache.coyote.tomcat4.CoyoteConnector (Apache)	[user.root]\oware\jboss-*.*\server\oware\deploy\jbossweb-tomcat41.sar\META-INF\ jboss-service.xml	app/medserver, jmx console, and web services, including Axis2
Other Ports			

Destination Ports	Service	Files	Notes
n/a[5](ICMP)	ping		MedSrv -> NtwkElement, NtwkElement -> MedSrv, ICMP ping for connection monitoring.
20[4, 5, 7] (TCP)	FTP Data Port	n/a Configurable in File Servers portlet editor	(Internally configurable), "MedSrv -> FTPSrv NtwkElement -> FTPSrv" medserver[1]
21[4, 5, 7] (TCP)	FTP Control Port	n/a	(Internally Configurable) "MedSrv -> FTPSrv NtwkElement -> FTPSrv" medserver[1]
22[4, 5, 7] (TCP)	SSH	n/a	MedSrv -> NtwkElement, secure craft access medserver[1]
23[4, 5, 7] (TCP)	Telnet	n/a	MedSrv -> NtwkElement, non-secure craft access medserver[1]
25 [4,5, 7] (TCP)	com.dorado.mbeans.OWEmailMBean (mail)	Configurable in the SMTP configuration editor in the Common Setup Tasks portlet.	AppSrv -> SmtpRelay, communication channel to email server from Appserver
69[4, 5, 7] (UDP)	TFTP	n/a	(Configurable internally), MedSrv -> TFTPSrv NtwkElement -> TFTPSrvmedserver[1]
161[4, 5, 7] (UDP)	com.dorado.mediation.snmp.request.listener.port (SNMP), oware.mediation.snmp.trap.forwarding.source.port	[user.root]\owareapps\ezmediation\lib\owmediation.properties	MedSrv -> NtwkElement, SNMP request listener and trap forwarding source medserver[1]
162[4, 5] (UDP)	oware.mediation.snmp.trap.forwarding.des tination.port (SNMP)	[user.root]\owareapps\ezmediation\lib\ezmediation.properties change this property: com.dorado.snmp.trap.listener.binding=0.0.0.0/162	NtwkElement -> MedSrv, SNMP trap forwarding destination port, medserver[1]
514[4, 5] (UDP)	com.dorado.mediation.syslog.port (syslog)	To change the syslog port, add com.dorado.mediation.syslog.port=[new port number] to owareapps\installprops\lib\installed.properties	NtwkElement -> MedSrv (mediation syslog port) medserver[1]
1098[4, 5, 7] (TCP)	org.jboss.naming.NamingService (JBOSS)	[user root]\oware\jboss-*.*\owareconf\jboss-root-service.xml	AppSrv -> MedSrv MedSrv -> AppSrv user client ->AppSrv user client ->MedSrv, (JBOSS naming service), app/medserver

Destination Ports	Service	Files	Notes
1099[4, 5, 7] (TCP)	org.jboss.naming.NamingService (JBOSS)	[user.root]\oware\jboss-*.*\owareconf\jboss-root-service.xml	MedSrv -> AppSrv, user client -> AppSrv, user client -> MedSrv, (JBOSS naming service & OWARE context server URL), app/medserver
1099[2, 4, 5, 7] (TCP)	OWARE.CONTEXT.SERVER.URL	[user.root]\oware apps\install props\lib\installed.properties [user.root]\oware apps\install props\medserver\lib\installed.properties	MedSrv -> AppSrv, user client -> AppSrv. user client -> MedSrv. (JBOSS naming service & OWARE context server URL) client medserver[1]
1100-1101	org.jboss.ha.jndi.HANamingService,	[user.root]/oware/jboss-*.*/server/all/deploy/cluster-service.xml	
1103[4, 5] (UDP)	jnp.reply.discoveryPort (JNP)	[user.root]\oware\lib\owappserver.properties	AppSrv -> MedSrv, AppSrv -> user client, (JNP reply discovery port), app/medserver
1123[4, 5] (UDP)	jnp.discoveryPort (JNP)	[user.root]\oware\lib\owappserver.properties	MedSrv -> AppSrv, user client -> AppSrv, (JNP discovery port), app/medserver
1521[4, 7] (TCP)	com.dorado.jdbc.database_name.oracle (JDBC)	[user.root]\oware apps\install props\lib\installed.properties	AppSrv ->OracleDBSrv, (JDBC database naming [Oracle]) database
3306[4, 7] (TCP)	com.dorado.jdbc.database_name.mysql	[user.root]\oware apps\install props\lib\installed.properties	AppSrv -> MySQLSrv, (JDBC database naming [MySQL]) appserver)
3100[4, 5, 7] (TCP) 3200[4, 5, 7]	org.jboss.ha.jndi.HANaming Service (JBOSS)	[user.root]\oware\jboss-*.*\owareconf\cluster-service.xml	AppSrv -> AppSrv, user client -> AppSrv AppSrv -> MedSrv MedSrv -> AppSrv user client -> AppSrv user client -> MedSrv (JBOSS HA JNDI HA Naming service [1100 is stub] app/medserver
3355[4] - application & mediation servers 8082 - portal	Direct access	Override application server port with this property: com.dorado.mediation.socket.relay.listen.port=3355	For both, the relay increments from the default until lit can bind to an open port.

Destination Ports	Service	Files	Notes
4444	org.jboss.invocation.jrmp.server.JRMPInvoker	[user.root]/oware/jboss-*.*/server/all/conf/jboss-service.xml, RMIObjectPort, jboss:service=invoker,type=jrmp	
4445[4, 5, 7] (TCP)	org.jboss.invocation.pooled.server.PooledInvoker (JBOSS)	[user.root]\oware\jboss-*.*\owareconf\jboss–root-service.xml	AppSrv -> MedSrv MedSrv -> AppSrv user client -> AppSrv user client -> MedSrv, app/medserver
4446[4, 5, 7] (TCP)	org.jboss.invocation.jrmp.server.JRMPInvoker (JBOSS)	[user.root]\oware\jboss-*.*\owareconf\jboss–root-service.xml	(AppSrv ->AppSrv, AppSrv -> MedSrv, MedSrv -> AppSrv, user client -> AppSrv, user client -> MedSrv) app/medserver
5988, 5989	WBEM Daemon (5989 is the secure port) defaults		You can add ports and daemons in monitored services. These are only the default. WBEM requires one port, and only one, per daemon.
6500-10[4, 5, 7] (TCP)	JBOSS	Specify such connections in the ezmediation/lib/ezmediation.properties file.	user client -> MedSrv (user client to mediation server cut-through)
7800[2](TCP)	org.jboss.ha.framework.server.ClusterPartition (JBOSS)	[user.root]\oware\conf\cluster-service.xml	disabled - see UDP for same, (JBOSS HA frame work server cluster partition) TCP only
8009 (TCP)	org.mortbay.http.ajp.AJP13Listener	[user.root]\oware\jboss-*.*\server\oware\deploy\jbossweb-tomcat41.sar\META-INF\ jboss-service.xml	Obsolete — appserver
8083 (TCP)	org.jboss.web.WebService (JBOSS)	[user.root]\oware\jboss-*.*\owareconf\jboss–root-service.xml	Used by JBoss web service, appserver
8093[4, 5. 7] (TCP)	org.jboss.mq.il.uil2.UILServerILService	[user.root]\oware\jboss-*.*\owareconf\uil2-service.xml	MedSrv -> AppSrv, user client -> AppSrv (JBOSS mq il uil2 UIL Server-IL Server), app/medserver (Jboss JMS)
8443[2,4, 5, 7]	org.apache.coyote.tomcat4.CoyoteConnector	[user.root]\oware\jboss-*.*\server\oware\deploy\jbossweb.sar\META-INF\ jboss-service.xml	user client -> AppSrv (Apache Coyote Tomcat4 Coyote connector), appserver. This is the default HTTPS port for the web portal.
9001[4, 6, 7] (UDP)	mediation.listener.multi cast.intercomm.port	[user.root]\lib\owmediation listeners.properties	MedSrv <-> MedSrv (mediation listener multicast intercommunications port) medserver[3]

Destination Ports	Service	Files	Notes
9996, 6343 (UDP)	Traffic Flow Analysis	trafficanalyzer.ocp	You must configure the router to send flow reports to the OpenManage Network Manager server on 6343 for sflow by default.
31310[4, 6, 7] (TCP)	JBoss		AppSrv -> AppSrv
45566[4, 5] (UDP)	org.jboss.ha.framework.server.ClusterPartition	[user.root]\jboss-*.*\owareconf\cluster-service.xml	AppSrv -> Multicast, (JBoss HA frame work server cluster partition), UDP only
54027[4,7]	Process Monitor	[user.root]\oware\lib\pmstartup.dat	mgmt client -> AppSrv, mgmt client -> MedSrv (process monitor local client for server stop/start/status) app/medserver

[1] Remote mediation servers or application servers behaving as though they were mediation servers (single host installation).

[2] Unused in standard configuration.

[3] Client does not connect to medserver on this port.

[4] This port is configurable.

[5]Firewall Impacting

[6]The most likely deployment scenarios will have all servers co-resident at the same physical location; as such, communications will not traverse through a firewall

[7]Bidirectional

To operate through a firewall, you may need to override default port assignments.

If you cluster your installation, you must disable multicast for communication through firewalls (to mediation servers or clients). Refer to the *OpenManage Network Manager Installation Guide* for more information.

NOTICE

To configure ports, open their file in a text editor and search for the default port number. Edit that, save the file and restart the application server and client. Make sure you change ports on all affected machines.

Note that mediation service also establishes a socket connection to client on ports 6500 to 6510 for cut through. Specify such port connections in the `ezmediation/lib/ezmediation.properties file`. (As always, best practice is to override when specifying properties.)

Finding Port Conflicts

You can find ports in use with the following command line:

```
netstat -a -b -o | findstr [port number]
```

Use this command to track down port conflicts if, for example, installation reports one. Best practice is to run OpenManage Network Manager on its own machine to avoid such conflicts.

Remote Mediation Ports

You must open the following ports between application servers and remote mediation servers: 8443, 3306, 3200, 7800, 8009, 8080, 9001, 31310, 45566.

Protocol Flows

The following network protocol flows represent the application's interactions with Network Devices (for example: Dell Powerconnect switches). The (N) in these lines identifies dynamic port assignments. Often, OpenManage Network Manager establishes several communication flows to a specified static port so N can represent several dynamic ports. This list also outlines alternative flows for JBoss JMS activation.

NOTE:

This does not identify time service flows like ntp that can manage the time on the servers.

The following were changes to a standard installation done for the sake of measuring the protocol flows. In the J2EE Naming Service: the RMIPort was changed to 31310. Also, `owappserver.properties` (turns off mediation v2 services on application server) was changed: mediation true->false. This essentially disables mediation on the application server.

The following is the installation that produced the listed protocol flows: Full Application Server Installation, Custom Mediation Installation, toggling off 2 (MySQL) and 5 (App Server). The client was a simple client installation.

Application Server to Mediation Server Flows

J2EE

TCP Med Svr (N) -> App Svr (1098)

TCP Med Svr (N) <-> App Svr (1098)

TCP Med Svr (N) -> App Svr (1099)

TCP Med Svr (N) <-> App Svr (1099)

TCP Med Svr (N) -> App Svr (4446)

TCP Med Svr (N) <-> App Svr (4446)

TCP Med Svr (N) -> App Svr (4445)

TCP Med Svr (N) <-> App Svr (4445)

JBoss JMS enabled:

TCP Med Svr (N) -> App Svr (8093)

TCP Med Svr (N) <-> App Svr (8093)

Application Server to Application Server in Application Server Cluster

IGMP App Svr-A/B -> 230.13.13.13 (Multicast address assigned per application cluster)
UDP App Svr-A/B (45566) -> 230.13.13.13 (45566)
IGMP App Svr-A/B -> 230.0.0.253

UDP App Svr-A/B (1123) -> 230.0.0.253 (1123)

UDP App Svr-A/B (1103) -> 230.0.0.5 (1103)

TCP App Svr-A (1100) <- App Svr-B (N)
TCP App Svr-A (1100) <-> App Svr-B (N)

TCP App Svr-A (31310) <- App Svr-B (N)
TCP App Svr-A (31310) <-> App Svr-B (N)
(Dynamic Port statically defined to be 31310 in the `cluster-service.xml` property file)

TCP App Svr-A (4446) <- App Svr-B (N)
TCP App Svr-A (4446) <-> App Svr-B (N)

TCP App Svr-A (2507) <- App Svr-B (N)
TCP App Svr-A (2507) <-> App Svr-B (N)

TCP App Svr-A (2508) <- App Svr-B (N)
TCP App Svr-A (2508) <-> App Svr-B (N)

TCP App Svr-B (N) -> App Svr-A (8080)
TCP App Svr-B (N) <-> App Svr-A (8080)

Application Server to Oracle Database Server

Optionally configured
TCP App Svr (N) -> Oracle DB Svr (1521)
TCP App Svr (N) <-> Oracle DB Svr (1521)

Application Server to MySQL Database Server

Embedded Database

TCP App Svr (N) -> MySQL Svr (3306)

TCP App Svr (N) <-> MySQL Svr (3306)

Mediation Server to Application Server Flows

J2EE

TCP App Svr (N) -> Med Server (4446)

TCP App Svr (N) <-> Med Server (4446)

TCP App Svr (N) -> Med Server (4445)

TCP App Svr (N) <-> Med Server (4445)

TCP App Svr (N) -> Med Server (1098)

TCP App Svr (N) <-> Med Server (1098)

Mediation Server uses 230.0.0.223:1123 to discover the application server cluster.

UDP Med Server (N) -> 230.0.0.223 (1123) (This multicast address is configurable)

UDP Med Svr (1123) -> 230.0.0.253 (1123)

Mediation Server to Mediation Server Flows

Mediation Server to Mediation Server cluster pair flows use the same ports to communicate between each other as those in the section Application Server to Application Server in Application Server Cluster on page 704. In addition, HA Trap processing use the following configurable multicast flow:

IGMP Med Svr-A/B -> 226.0.0.226

UDP Med Svr-A (9001) -> Med Svr-B (9001)

UDP Med Svr-A (9001) <-> Med Svr-B (9001)

Mediation Server to Network Element Flows

Telnet

TCP Med Server (N) -> Network Element (23)

TCP Med Server (N) <-> Network Element (23)

SSHv1/SSHv2

TCP Med Server (N) -> Network Element (22)

TCP Med Server (N) <-> Network Element (22)

FTP (mediation server FTPs files to and from the FTP server)

TCP Med Server (N) -> FTP/TFTP Svr (21)

TCP Med Server (N) <-> FTP/TFTP Svr (21)

TCP Med Server (N) <- FTP/TFTP Svr (20)

TCP Med Server (N) <-> FTP/TFTP Svr (20)

TFTP

Not applicable

SNMP

UDP Med Server (162) <- Network Element (N) (trap receipt)

UDP Med Server (N) -> Network Element (161) (get/set)

UDP Med Server (N) <- Network Element (161)

ICMP

No ports are involved with ICMP, but you must allow ICMP traffic from the application/ mediation server and devices (and back).

Syslog

UDP Med Server (514) <- Network Element (514) (syslog messages) (TCP is possible but not implemented)

Mediation Server to FTP/TFTP Server

TCP (N) -> FTP/TFTP Svr (21) (ftp-control)

TCP (N) <-> FTP/TFTP Svr (21)

TCP (N) <- FTP/TFTP Svr (20) (ftp-data)

TCP (N) <-> FTP/TFTP Svr (20)

TCP Med Svr (N) -> FTP/TFTP Svr (69) (Testing "File Server")

TCP Med Svr (N) <-> FTP/TFTP Svr (M)

Mediation Server to Trap Forwarding Destination

IP Trap Forwarding

Network Element (161) -> Trap Forwarding Receiver (statically defined N ex. 162 UDP)

NOTE:

The forwarded trap actually has the IP address of the Network Element, not the Med Server.

Network Element to FTP/TFTP Server

FTP

Network Element (N) -> FTP/TFTP Svr (21)

Network Element (N) <-> FTP/TFTP Svr (21)

Network Element (N) <- FTP/TFTP Svr (20)

Network Element (N) <-> FTP/TFTP Svr (20)

Network Element (N) -> FTP/TFTP Svr (69)

Network Element (N) <-> FTP/TFTP Svr (M)

Devices should have connectivity to the external FTP/TFTP server. *M* means we recommend installing external file servers on mediation servers for a performance improvement. You can also use the internal FTP/TFTP server in Windows environments.

Client to Application Server

J2EE

TCP RC clt (N) -> App Svr (1099)

TCP RC clt (N) <-> App Svr (1099)

TCP RC clt (N) -> App Svr (1098)

TCP RC clt (N) <-> App Svr (1098)

TCP RC clt (N) -> App Svr (4446)

TCP RC clt (N) <-> App Svr (4446)

TCP RC clt (N) -> App Svr (4445)

TCP RC clt (N) <-> App Svr (4445)

IGMP RC clt(N) -> 230.0.0.5

UDP RC clt(1123) -> 230.0.0.253 (1123)

UDP RC clt(1103) <- App Svr(1103)

TCP RC clt (N) -> App Svr (1100)

TCP RC clt (N) <-> App Svr (1100)

JBoss JMS enabled:

TCP RC clt (N) -> App Svr (8093)

TCP RC clt (N) <-> App Svr (8093)

Client to Mediation Server (Direct Access, or Cut thru)

Telnet/SSHv1/SSHv2 Cut - through

RC clt (N) -> Med Svr (1099)

RC clt (N) <-> Med Svr (1099)

RC clt (N) -> Med Svr (1098)

RC clt (N) <-> Med Svr (1098)

RC clt (N) -> Med Svr (4446)

RC clt (N) <-> Med Svr (4446)

RC clt (N) -> Med Svr (4445)

RC clt (N) <-> Med Svr (4445)

RC clt (6500) <- Med Svr (N) (6500 represents ports 6500-6510)

RC clt (6500) <-> Med Svr (N)

Email Network Element Config Differences

If email from the application server is turned on then the following port must be opened between the application and email server:

TCP App Svr (N) -> smtp relay (25)

TCP App Svr (N) <-> smtp relay (25)

JBoss Management Access

The J2EE server has port 8080 open to allow web browsers access to the JBoss Management console. If you want to access this capability then the system browsing the jmx console must have access.

Mgmt client (N) -> App Server (8080)

To access the Mediation Servers:

Mgmt client (N) -> Med Server (8080)

Ports and Application To Exclude from Firewall

Exclude `java.exe`, tcp port 21 and udp port 69 from firewall interference to let the application function. The java process to exclude from firewall blocking is `<Installdir>\oware3rd\jdk[version number]\jre\bin\java.exe`.

If you have distributed the database functions then you must allow the database process to communicate with your machine through your firewall as well. The embedded database process is `mysqld-max-nt.exe` (in Windows, the path is `<installdir>oware3rd\mysql\[version number]\bin\mysql-max-nt.exe`). Consult your DBA for Oracle processes, if applicable.

Firewall Configuration

Example Linux firewall configuration (from `iptables-save > my-config-file`):

```
-A INPUT -p tcp -m state --state NEW -m tcp --dport 21 -j ACCEPT
```

```
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -p udp -m state --state NEW -m udp --dport 69 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 161 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 162 -j ACCEPT
-A INPUT -p udp -m state --state NEW -m udp --dport 162 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 514 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 1099 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 1100 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 1101 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 3306 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 8089 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 5900 -j ACCEPT
-A INPUT -p udp -m state --state NEW -m udp --dport 5900 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 6343 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 8080 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 8089 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 8082 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 8083 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 8119 -j ACCEPT
-A INPUT -p udp -m state --state NEW -m udp --dport 8162 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 8162 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 9996 -j ACCEPT
-A INPUT -p udp -m state --state NEW -m udp --dport 9996 -j ACCEPT
```

Add any new lines to the firewall file `/etc/sysconfig/iptables`, and restart the firewall service.

Installed Third Party Applications

This software includes the following applications. License information follows in parenthesis:

ant (licensed under GNU Lesser General Public License [LGPL] http://www.gnu.org/licenses/)

cygwin (LGPL)

expect (Public Domain)

J Free Charts (LGPL)

Jasper Reports (LGPL)

JBoss (see directory name for version) (LGPL)

JDK (Open Source)

JLoox — (Commercially Licensed to this vendor, not re-distributable)

MySQL — (GNU Public License [GPL])

Open SSH — includes OpenSSL (LGPL)

OpenLDAP — (OpenLDAP License: http://www.openldap.org/software/release/license.html)

Perl — (LGPL)

TCL — (LGPL)

Tomcat — (Apache License)

Liferay Portal—Liferay Community Edition (LGPL)

The LGPL, GPL and Apache licenses let us redistribute the above listed open source components, but the EULA for all OpenManage Network Manager products prohibits redistribution of any package or component of the software. Consult the product's EULA.htm file, typically in the `InstData` directory of the installation source for more information.

Windows Management Instrumentation Ports

Windows Management Instrumentation uses the following ports:

Protocol or Function	Ports Used
RPC, TCP	135,139,445,593
SNMP, UDP	161,162
Optional:	
WINS, TCP	42
UDP	42, 137
PrintSpooler, TCP	139, 445
TCP/IP PrintServer, TCP	515

These are relevant only if you are using any Windows-based server device driver.

Glossary

ACCESS CONTROL — Refers to mechanisms and policies that restrict access to computer resources. An access control list (ACL), for example, specifies what operations different users can perform on specific files and directories.

ALARM — A signal alerting the user to an error or fault. Alarms are produced by events. Alarms produce a message within the Alarm Window.

API — Application Programing Interface—A set of routines used by the application to direct the performance of procedures by the computer's operating system.

AUTHENTICATION — The process of determining the identity of a user that is attempting to access a network. Authentication occurs through challenge/response, time-based code sequences or other techniques. See CHAP and PAP.

AUTHORIZATION — The process of determining what types of activities or access are permitted on a network. Usually used in the context of authentication: once you have authenticated a user, they may be authorized to have access to a specific service.

COS — Class of Service—Describes the level of service provided to a user. Also provides a way of managing traffic in a network by grouping similar types of traffic.

DATABASE — An organized collection of Oware objects.

DEPLOYMENT — The distribution of solution blades throughout the domain.

DIGITAL CERTIFICATE — A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting and decrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

DOMAIN — A goal-oriented environment that can include an industry, company, or department. You can use Oware to create solutions within your particular domain.

ENCRYPTION — Scrambling data in such a way that it can only be unscrambled through the application of the correct cryptographic key.

EQUIPMENT — A network device managed by the system.

ETHERNET TRUNK — An Ethernet Trunk service represents a point-to-point connection between two ports of two devices. Ethernet frames transported by the connection are encapsulated according to IEEE 802.1Q protocol. The each tag ID value in 802.1Q encapsulated Ethernet frames distinguishes an Ethernet traffic flow. Thus, an Ethernet trunk can aggregate multiple Ethernet VLANs through a same connection which is why "trunk" describes these.

ETHERNET TRUNK PORT — An Ethernet trunk port is a port that terminates a point-to-point Ethernet trunk. Since Ethernet trunk is a point-to-point connection, each Ethernet trunk contains two Ethernet trunk ports.

ETHERNET SERVICE — An Ethernet service represents a virtual layer broadcast domain that transports or transmits Ethernet traffic entering from any one endpoint to all other endpoints.

Often, this is a VLAN service across multiple devices.

An Ethernet service may or may not use Ethernet trunk, depending on the desired connection between two neighboring devices. If the connection is exclusively used for this Ethernet service, no Ethernet trunk is needed. On the other hand, if the connection is configured as an aggregation which can be shared by multiple Ethernet services, an Ethernet trunk models such a configuration.

Each Ethernet service can have multiple Ethernet Access Ports through which Ethernet traffic flows get access to the service.

ETHERNET ACCESS SERVICE — Since an Ethernet trunk can be shared by multiple Ethernet Services, each Ethernet Service relates to a shared trunk via a unique Ethernet Access component.

Because Ethernet trunk is a point-to-point connection, there are two Ethernet Access Services per trunk per Ethernet service instance.

ETHERNET ACCESS POINT — These represent the access points through which Ethernet frames flow in and out of an Ethernet service.

For an Ethernet Service that uses an Ethernet Trunk Service, an Ethernet Access Port must be associated with either one of the two Ethernet Access Services.

EVENT — Notification received from the NMS (Network Management System). Notifications may originate from the traps of network devices or may indicate an occurrence such as the closing of a form. Events have the potential of becoming alarms.

EVENT DEFINITION — Parameters that define what an event does. For example, you can tell Oware that the event should be to wait for incoming data from a remote database, then have the Oware application perform a certain action after it receives the data.

EVENT INSTANCE — A notification sent between two Oware components. An event instance is the action the event performs per the event definition.

EVENT TEMPLATE — Defines how an event is going to be handled.

EVENT THRESHOLD — Number of events within a given tomfooleries that must occur before an alarm is raised.

EXPORTING — Saving business objects, packages, or solution blades to a file for others to import.

Filter — In network security, a filter is a program or section of code that is designed to examine each input or output request for certain qualifying criteria and then process or forward it accordingly.

GUI — Graphical User Interface

ISATAP — The Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) is an IPv6 transition mechanism which is defined as a tunneling IPv6 interface and is meant to transmit IPv6 packets between dual-stack nodes on top of an IPv4 network.

Key — In cryptography, a key is a variable value that is applied using an algorithm to a string or block of unencrypted text to produce encrypted text. The length of the key generally determines how difficult it will be to decrypt the text in a given message.

Key Management — The establishment and enforcement of message encryption and authentication procedures, in order to provide privacy-enhanced mail (PEM) services for electronic mail transfer over the Internet.

Managed Object — A network device managed by the system.

Mediation — Communication between this application and external systems or devices, for example, printers. Mediation services let this application treat these devices as objects.

Mediation Agent — Any communication to and from equipment is handled by the Mediation Agent. This communication includes SNMP requests, ASCII requests, and unsolicited ASCII messages. In addition, the Mediation Agent receives and translates emitted SNMP traps and converts them into events.

MEG — Maintenance Entity Group

MEP — Maintenance End Point

MIB — Management Information Base. A database (repository) of equipment containing object characteristics and parameters that can be monitored by the network management system.

OAM — Operation, Administration and Maintenance

OID — Object ID.

OSPF — Open Shortest Path First routing protocol.

Policy — A rule made up of conditions and actions and associated with a profile. Policy objects contain business rules for performing configuration changes in the network for controlling Quality of Service and Access to network resources. Policy can be extended to perform other configuration functions, including routing behavior, VLAN membership, and VPN security.

Policy Enforcement Points (PEP) — In a policy enforced network, a policy enforcement point represents a security appliance used to protect one or more endpoints. PEPs are also points for monitoring the health and status of a network. PEPs are generally members of a policy group.

POLICY ROUTING — Routing scheme that forwards packets to specific interfaces based on user-configured policies. Such policies might specify that traffic sent from a particular network should be routed through interface, while all other traffic should be routed through another interface.

POLICY RULES — In a policy enforced network (PEN), policy rules determine how the members and endpoint groups of a policy group communicate.

PPTP (POINT-TO-POINT TUNNELING PROTOCOL) — Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a virtual private network (VPN) across TCP/IP-based data networks. PPTP supports on-demand, multi-protocol, virtual private networking over public networks, such as the Internet.

PRIVATE KEY — In cryptography, a private or secret key is an encryption/decryption key known only to the party or parties that exchange secret messages. In traditional secret key cryptography, a key would be shared by the communicators so that each could encrypt and decrypt messages. The risk in this system is that if either party loses the key or it is stolen, the system is broken. A more recent alternative is to use a combination of public and private keys. In this system, a public key is used together with a private key.

PROFILE — A profile is an abstract collection of configuration data that is utilized as a template to specify configuration parameters to be applied to a device as a result of a policy condition being true.

PUBLIC KEY — A public key is a value provided by some designated authority as a key that, combined with a private key derived from the public key, can be used to effectively encrypt and decrypt messages and digital signatures. The use of combined public and private keys is known as asymmetric encryption. A system for using public keys is called a public key infrastructure (PKI).

QOS — Quality of Service. In digital circuits, it is a measure of specific error conditions as compared with a standard. The establishment of QoS levels means that transmission rates, error rates, and other characteristics can be measured, improved, and, to some extent, guaranteed in advance. Often related to Class of Service (CoS).

RADIUS — RADIUS (Remote Authentication Dial-In User Service) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share.

RIP — Routing Information Protocol

SELF-SIGNED CERTIFICATE

A self-signed certificate uses its own certificate request as a signature rather than the signature of a CA. A self-signed certificate will not provide the same functionality as a CA-signed certificate. A self-signed certificate will not be automatically recognized by users' browsers,

and a self-signed certificate does not provide any guarantee concerning the identity of the organization that is providing the website.

SMTP — Simple Mail Transfer Protocol.

SNMP — Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides the means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

Spanning Tree Protocol (STP) — The inactivation of links between networks so that information packets are channeled along one route and will not search endlessly for a destination.

SSH (Secure Shell) — A protocol which permits secure remote access over a network from one computer to another. SSH negotiates and establishes an encrypted connection between an SSH client and an SSH server.

SSL (Secure Sockets Layer) — A program layer created by Netscape for managing the security of message transmissions in a network. Netscape's idea is that the programming for keeping your messages confidential ought to be contained in a program layer between an application (such as your Web browser or HTTP) and the Internet's TCP/IP layers. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer.

Trap (SNMP Trap) — A notification from a network element or device of its status, such as a server startup. This notification is sent by an SNMP agent to a Network Management System (NMS) where it is translated into an event by the Mediation Agent.

Trap Forwarding — The process of re-emitting trap events to remote hosts. Trap Forwarding is available from the application through Actions and through the Resource Manager.

VLAN — A virtual local area network (LAN), commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the Broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. Network reconfiguration can be done through software instead of physically relocating devices.

Index

A

Access Control 711
Access Profile
  General 366
  Template Editor 365
  Templates 364
  Templates Portlet 354
Action Group Editor 315
Action Groups 315
Action Job Screen Results panel 287
Actions 492
  initiating from topology view 147
actions
  scheduling 90
Actions in Visualizations 524
Active Directory 42
Active Performance Monitor
  Create ACLI 190
  Show Command 189
  SNMP Performance Monitoring 186
  SNMP Performance Monitoring Example 186
  Support 309
Adaptive CLI
  Actions 265
  Attribute Appearance and Validation 284
  Attribute Presentation 278
  Attributes 272
  Conditional Blocks 291
  Continue Pattern 281
  Editor 270
  Error Condition 281
  Example extracting Upload / Download Speeds 300
  General 270
  Juniper E-Series 270
  Juniper M/T 270
  Login limitations 263
  Monitor Attributes 310
  Non Configuration attributes 280
  Perl Scripts 291
  Prerequisite Validation 282
  Script Language Syntax 290
  Scripts 278
  Setting devices to configuration mode 270
  Troubleshooting 317
  Troubleshooting Timeouts 317
  With Reboot 297
Adaptive CLI FAQs 413
Add > Applications menu 50
Add a Windows Firewall Exception for Remote WMI Connections 402
Adding or Updating Extensions 417
Additional Products 18
Additional WMI Troubleshooting 402
Advanced External Script Monitor 311
advanced filters
  defining 86
Advanced Troubleshooting 381
Aging Policies
  Editor 691
  Options 693
Alarm 711
Alarm / Performance / Database 386
Alarm / Performance / Retention 386
Alarm archiving 38, 681
Alarm Life Cycle 125
Alarm Processing Flow 125
Alarm Propagation, enhanced 636
Alarm Suppression in Topology Views 530
Alarms
  Alarm State 476
  Assigned User 476
  Correlation, Parent/Child 479
  Date Assigned 476
  Date Closed 476
  Date Opened 474, 570
  Editor 481
  Email 480
  Entity Type 474, 481
  In Topology 530
  Notification Instance 476
  Service Effecting 475
  service effecting 571, 606
  Snap Panels 478
  Visualizations / Topologies 530
Alarms / Monitors / Performance 380
Alarms portlet
  disable context 144
Amigopod 70
AP Editor / AP Template Editor 365

API 711
Application Server
Statistics 167
Application Server Does Not Start 375
Application Server Memory (Linux) 405
Application Server Memory Low 405
Application Server Status Monitor 185
Application Settings 686
Archiving data 38, 681
Aruba
Backup and Restore 409
Backup and Restore limitations 409
Devices 409
SNMP limitations 409
Aruba Devices 409
Associate Contact to Equipment 141
Attribute Presentation 278
Attributes
Alternative ways of Grouping in Reports 620
Attributes Extraction 283
Audible Alerts 94
Audit Trail
Screen 689
Snap Panels 632
Audit Trail portlet 631
Authentication 73, 711
Authoritative User 364
Authorization 711
Authorizations 508
Automation rules 489
Avaya
Cut-Through 410
Device Prerequisites 409
RTCP 410
Setting Up RTCP 410
Avaya Device Prerequisites 409
Avoiding restore for trivial differences 322

B

Background Settings 528
Backup / Restore / Deploy 380
Backup and Restore 409
Backup/Restore/Deploy 385
Backups
Configurations 151
Latest Configurations 222
Bandwidth Calculation 216
banners, characters in 61
Base Driver 66
Basic Network Considerations 25
Best Practices
FTP Servers 150
MySQL configuration 74
Overriding Properties 71
Performance and Monitors 157
Refresh Proscan Targets 599
Report size limitations 614
System Repair / Maintenance 76
Web portal / Multitasking 24
BIG-IP F5 412
Brocade Devices 411

C

Calculating bandwidth 216
Calculations within Top N Portlets 220, 536
CAS 44
Central Authentication Server 44
Central Authentication Server (CAS) 44
Change Determination Process 346
Change Management / ProScan 321
Change Manager
Compliance Policy Violation report 324
Use paradigms 321
Change the site logo 677
Changing Dashboard Time / Date Format 225
Cisco
Copying to the Device Rather than the Application 413
Devices 412
Event Processing Rules 343
IOS upgrade caveat 413
IPSLA Monitoring 197
Proscan Policy Groups 341
Saving Running-Config to Startup Config 413
Setup Prerequisites 412
Cisco Compliance
Actions 342
Policies 340
Cisco Devices 412
Cisco Metro Ethernet SLA Monitors 200
Clustering 416
columns
modifying settings 85
Common Device Prerequisites 408
Common Problems 383
Common Setup Tasks 625
Communication Problems 383
Comparison reports 619
Compliance Policy Summary 324
Conferences 445
Configuration Files 579
Editor 585
Configuration Files portlet not visible 681

configuration management portlets
File Servers 593
Configure Alarm E-mail 478
Configure Distributed Component Object Model (DCOM) and User Account Control (UAC) 399
Configuring
Multitenancy 354
Configuring Audit Trails 89
Configuring Chat for Multitenancy 353
Configuring Job Viewer 89
Configuring Monitors 157
Configuring Pages and User Access 47
Configuring Resync 62
Constraining Data Access 368
Contacts
Editor 649
Portlet 426, 618, 647
Container
Authorizations 508
General 507
Membership 508
Multitenancy 506
Portlets filtered 510
With Maps 664
Container Editor
General 507
Container Manager
Expanded 506
Container View
Multitenant Sites 511
containers
understanding 144
using 145
context
disabling Alarms portlet response 144
display rules 144
Continue Pattern 281
Control Center
Administrator options 674
Control Panel
Server Administration > Mail 32, 65
Cookies and Sessions 24
Copying to the Device Rather than the application 413
CoS 711
Create the Monitor 192
creating
topology view 147
creating users 49
CRON Events 415
Custom Action 494
Custom Attributes 682
Custom Debug 82
Custom Report Images 132
Customizing Report Logos 132
Cut-Through 410

D

DAP 38, 681
SubPolicies 692
viewer 695
Dashboard
Editor 227
Time / Date Format 225
View Selection 226
Views 223
Dashboard Performance 160
Dashboard Templates for Interface and Port Equipment 235
Data Configuration 682
Data rollup 174, 223
Data summary 174
Database 711
Database Aging
Policies 681
Sub-Policies 693
Database Backup 39
database sizing 73
Date format 59, 553
Debug 391
Default Server Status Monitor 185
Default User Roles 676
Deploying firmware fails 385
Deployment 711
Device O/S Overrides 385
Device Prerequisites 406
Digital Certificate 711
Direct Access
Tool 550
Direct Access Fails Because of Java Security Settings 377
Disabling Remote User Account Control for Workgroups 401
Discovery
exclude IP addresses 60
Discovery / Resync 380
Discovery Issues 384
Discovery Profile
Inspection 61
Network 60
Results 62
Display Strategies 524
Displaying Tenant Domains in Top N Portlets 222
DNS 25
DNS Does Not Resolve Public Addresses 416
Domain 711
Domain Access 368
Domain, Name Servers 25
Domains 674
drvrpt 672

E

Edit Custom Attributes 88
editors
External File Server 594

Email Action 495
Variables 100
e-mail reply 627
e-mail sender 627
E-mail variables 100
Enable Remote Procedure Call (RPC) 398
Enabling Account Privileges in WMI 400
Enabling DCOM 399
Enabling Estimated Flows 240
Encryption 711
Enhanced Alarm Propagation 636
Environment / Operating System Issues 415
Equipment 711
Name 476
Error Condition 281
Ethernet Access Point 712
Ethernet Access Service 712
Ethernet Service 712
Ethernet Trunk 711
Ethernet Trunk Port 712
Event 712
Child 114
Messages 502
Event Definition 712
Event Definitions 114
Correlations 502
Editor 498
Extensions 504
General 498
Message Template 500
Event History
Portlet 482
Snap Panels 484
Event Instance 712
Event Life Cycle 122
Event Processing
Filters 486
Rules 95
Event Processing Flow 122
Event Template 712
Event Threshold 712
Expanded
Actions Portlet 266
Alarm Portlet 475
Audit Trail Portlet 632
Event History Portlet 483
Location Portlet 646
Portlets 450
Reports Portlet 615
Resource Monitor 171
Vendor Portlet 644
Export / Import
Page Configurations 87
Exporter Registration 247
Exporting 712
exporting
topology views to Visio 148
Extended Event Definitions (EED) 114, 115
extending topology Label Length 147
External File Server editory 594
External Script Monitor
Advanced 311
Extract an Adaptive CLI Attributes from a Syslog Alarm 104

F

Fail to Connect Application Server / Client 379
FAQ
Adaptive CLI 413
Backup and Restore 409
Debug fine tuning 392
Discovery Problems 383
Log Generation Fails with "Build Failed" Error (Linux) 395
Monitoring Mediation Servers 403
Prevent discovery problems 383
Radius Authentication Alternatives 44
Resolve port conflicts 393
Troubleshooting 371
Unix issues 404
WMI Troubleshooting 395, 396
FAQs
LDAP 44
File
Backup, Restore 584
Management 582
File Issues 373
File Servers
Port conflict 627
File Servers portlet 593
Filter 19, 713
Management 685
Visualize portlet 517
Filter / Settings (Rule Editor) 486
Finding Port Conflicts 393, 702
Fine Tuning Event Messages 502
Fine-Tuning Debug 392
Firewall 708
Issues 68
Requirements 28
Firewall Configuration 708
Fixed IP Address 26
Flipdebug 392
Formatting reports 130
Forward Northbound 497
Forwarding Configuration Change Commands 350
FTP
Protocol Selection 627
Servers 151
FTP server 150
Functional permissions 680

G

General (Rule Editor) 485
Generic Trap 98
getlogs 394
Google maps, setting up 145
Group File Management Failure 386
Group Reports 133
GUI 713

H

Hardware 381
Hardware Errors 415
Hardware sizing
  Cloud Server 160
Heap
  Tuning Advice 72
Heartbleed SSL vulnerability 30
How to
  Add User Roles 34
  Add Users 32
  Advanced Script Monitor Example 311
  Backup Configurations 151
  Configure an Action Group 316
  Configure ProScan Groups 322
  Configure User Site Access 367
  Create a Container for each Customer 51
  Create a Custom Dashboard View 228
  Create a Key Metrics Monitor 188
  Create a Monitor for an External Script 192, 310
  Create a Multitenancy Environment 355
  Create a new Page Tab (My Resources) 49
  Create A Performance Template 233
  Create a Report Template 130
  Create a Server Status Monitor Dashboard 186
  Create a Simple Dashboard View 225
  Create an Adaptive CLI Monitor 189
  Create an ICMP Monitor 188
  Create an SNMP Interface Monitor 186
  Create Event Processing Rules 95
  Create Source Group Criteria 330
  DAP Workflow 682
  Deploy an OS Image 154
  Discover Your Network 59
  Do Change Management (Example) 323
  Make an Adaptive CLI Run an External Script 289
  Make an LDAP Admin User 37
  Monitor Network Availability 173
  Open an archived file in dapviewer. 39
  Report on Change Determination 349
  Restore a single configuration to many target devices 154
  Restore Configurations 152
  Run Change Determination Process 346
  Use “How To” 20
  Use Extended Event Definitions 114
  Use Traffic Flow Analyzer 246
  View Historical Dashboard Data 232
HTTP Authentication 385
HTTPS 28

I

ICMP (Ping) 383
ICMP Monitor 207
Incomplete Discovery 62
Increasing Startup Logging 394
Initial Logon after installation fails 377
Installation Issues 373
Installer Failure 375
Installer Logs 375
Install-From Directory 375
Interface Portlet 545
Interfaces connected to customers. 141
Internal FTP server limitations 150
IP Address changes 26
IP v4 / v6 55
IPSLA OIDS 197
ISATAP 713

J

Java 708
Jstack Debugging in Windows 7 403
Juniper COS 208
Juniper RPM 209
Juniper XE Devices 239

K

Key 713
Key Features 17
Key Management 713
Key Metric
  Editor 236
  Monitor 210

L

Labels 583
LDAP 36, 41
LDAP FAQs 44
Legend Tab 528
License 19
  Viewer 653
license expiration warning 654
License Expiration Warning Alarms 53, 658
License Installation 418
Licenses
  Traffic flow 239, 387
Linked View 521
Links
  Visualization 531
Linux Firewall
  Turn off 380
Linux Issues 404
lists of
  portlet tools and options 448
LLDP Warnings in Discovery 62
Localization 33
Location
  Editor 645
  Manager
    Address 646
    Parent location 645
  Portlets 644
  Snap Panels 646
  Updates 512, 647
Log
  Categories 392
  Retention 394
Log Generation Fails with "Build Failed" Error (Linux) 395
Login
  Failures 379
  Restrictions 359
Logon Fails with Invalid Logon Message 377
Logs 394
logs.jar 394

M

Mail hosts 677
Maintenance
  CLI Trace Debug logs 78
  Database Aging Policies (DAP) 78, 373
  Database Backup 78
  Scheduled Items 78
Manage > Domain Access 368
Managed Object 713
Mandatory Fields 448
Map Context 662
  Portlets filtered 510
  With Containers 664
  Without Containers 663
maps
  setting up Google maps 145
  setting up Nokia maps 146
Maps and Containers Together 664
Mass deployments 590
Match Regex for each line 328
Mediation 683, 713
  Server Status Monitor 185
Mediation Agent 713
Mediation Server on separate machine fails 378
MEG 713
Memory
  Advice 72
  Tuning 72
Memory Issues 406
Memory issues
  Windows heap 406
Menu 477
MEP 713
MIB 713
MIB Browser
  Tool 550
  Undiscovered devices 212
MIB File locations 550
Migrating
  Heartbeats 178
Missing Performance Data / Monitor Stops Polling 388
Monitor
  Discovery Relationship 157
  Graph Background 183
  Options Type-Specific Panels 196
  Reports in Multitenant Environments 189
  Strings 303
  Text Values 303
  Top N 220
Monitor Editor 176
  Calculated Metrics 179
  Conditions 184
  Inventory Mappings 183
  Monitor Options 179
  Thresholds 181
Monitor Life Cycle 162
monitorAttributeTrend 123
Monitoring from a Cloud Server 160
Monitoring Life Cycle 162
monitorTargetDown 160
More Failures on Startup 378
MSP 674
Multiple indexes in the SNMP Interface 214

Multiple Performance Templates 235
Multitenancy 674
Access Profile Editor General 366
Access Profile Template Editor 365
Access Profile Templates 364
Access Profile Templates Portlet 354
Assigning Devices in Discovery 357
Authoritative User 364
Batch Imports 353
Chat 353
Components 354
Configuring page access 358
Constraining Data Access 368
Containers 506
Control Panel 354
Creating a Site Template 355
Creating an Access Profile Template 356
Creating Sites 359
Discovery Profiles Portlet 354
Displaying Tenant Domains in Top N Portlets 222
Domain Access 368
Event Processing Rules (EPRs) 512
General 366
Importing Discovery Profiles 58, 553
Login Restrictions 359
Manage > Domain Access 368
Managed Resources Portlet 354
Multitenant Batch Imports 353
Organization Settings 363
Page Templates 362
Portal > Page Templates 362
Portal > Site Templates 360
Portal > Sites 359
Provisioning Site-Creating User Permissions 355
Resource Access 368
Resource Assignments 366
Roles 676
Roles and permissions 676
Serving Multiple Customer Accounts 353
Site Id Filtering 369
Site Management 358
Site Management and Access Profiles 354
Site Management Editor 363
Site Management Portlet 354
Site Templates 360
Sites 359
Sites / Site Templates in Control Panel 359
Supported Portlets 357
Template Association 366
User Site Access 366
User Site Access Policy 367
User Site Access Portlet 354
View and Further Configure Devices for the Site 356
Multitenancy and LDAP 44
Multitenant Users 36
my.cnf 73
MySQL
Changing InnoDB Log Files 76
Optimizing 73
MySQL Database Issues 390
MySQL Database Sizing 73

N

Name Resolution 25
Netrestore File Servers 627
Network
Basics 25
Considerations 25
Monitoring 387
Requirements 25
Topology 516
Network Assessor Reports 136
Network Tools 549
Direct Access 550
MIB Browser 550
Ping 549
New permissions 681
NFV user interface
Settings window 451
Nokia maps, setting up 146
Non Configuration attributes 280
Northbound Generic trap 98
NTLM 44

O

OAM 713
OID 713
Open SSO 44
OpenID 44
Oracle Database Issues 391
Organization Settings 363
OSPF 713
Portal > 678
Other Failures on Startup 378
Other Installation Issues 374

P

Page Locations 443
page navigation bar 443

page-level permissions 50
Partition Name Limitations 26
Password Policies 677
Password reminder disable 28
Password Reset 65
Patch Installation 417
Patches 391
Performance and Monitors 157
Performance Dashboard 226
  Portlet 226
Performance Monitor Flow 162
Performance Note 20
Performance Tuning Traffic Flow Analysis 240
Perl
  Perl Script Example 292
Perl / Java (Groovy) Language Policies 335
Permissions
  Manager 678
permissions
  setting page-level 50
  setting portlet-level 51
  setting resource-level 51
Personal pages 48
Ping Tool 549
pmtray 27
Policy 713
Policy Enforcement Points (PEP) 713
Policy routing 714
Policy Rules 714
Portal
  Memory Settings 72, 416
  Portal Settings 677
  Roles 676
  Settings 677
Portal > Password Policies 677
Portal > Sites / Site Templates in Control Panel 359
Portal Updates (netview.war) 417
Portlet 447
  Instances 453
portlet
  permissions 51
portlets
  Audit Trail 631
  maximized view 448
  refreshing 449
  tools and options 448
Ports
  Assignments 698
  Expanded 544
  Required 28
  Used 698
Ports connected to customers 141
Post Upgrade Web Portal Problems 416
Potential Problem Processes 415
PPTP (Point-to-Point Tunneling Protocol) 714
Pre-Flight Checklist 373
Preventing Discovery Problems 383
printing a portlet's contents 447
Private Key 714
Profile 714
Promote 590
Propagation
  Ports v. Devices 499
ProScan 321, 562
  Case Sensitive 330
  Compliance Reporting 349
  count number of occurrences 329
  Criteria Properties 330
  Editor 325
  Editor - Compliance 327
  Editor - General 325
  Java (Groovy) 337
  Manager 324, 597
  Monitor 211
  Multi-Line Support 330
  Perl 336
  Policy, Group Editor 339
  Supported Regular Expressions 333
  Use Cases 321
  Use paradigms 321
ProScan Policy
  Creating or Modifying 325
  Creating or Modifying Groups 339
Protocol
  Flows 703
Protocol Flows 703
Public / Private Page Behavior 676
Public Key 714

Q

QoS 714
QoS C3pl Account Monitor 206
Qos Class Map Monitor 202
Qos Estimate Bandwidth Monitor 206
Qos IPHC Monitor 205
Qos Match Statement Monitor 203
Qos Packet Marking Monitor 205
QoS Police Monitor 205
Qos Police Monitor 203
Qos Queuing Monitor 203
Qos RED Monitor 204
Qos Traffic-Shaping Monitor 204
Quick Navigation portlet 471

R

RADIUS 44, 714
Raise User Limits 416
Recommended Windows File Servers 151
Redcell > Application Settings 686

Redcell > Mediation 683
redcellUnknownTrap 634
Refresh Monitor Targets 218
refresh tool 449
Regular Expression metacharacters 333
Regular Expressions 333
metacharacters 307
Special characters 307
re-index 674
Re-indexing Search Indexes 382
Remote Mediation Ports 703
Report Missing Data 388
Report Templates
Editors 618
Reports 388
Customizing Logos 132
formatting 130
Maximum size 612
Portlet 131
Snap Panels 616
Repositories 694
Reset the WMI Counters 397
Resize columns 447
Resolving Port Conflicts 393
Resource Assignments 366
Resource Discovery 138
Resource Management
Portlet 562
Resource Monitors
Portlet 169
Snap Panels 172
resource-level permissions 51
resources
sharing 87
Restore Configurations 152
Restoring Compliant Files 322
Restoring Database 40
Resync 62
Resync alarms 478
Retention Policies 174, 387
return address 627
Return to previous 449
revision history (guide) 21
RIP 714
Roles 676
RTCP 410
Rule Editor 484
Actions 492

S

Saving page configurations 48
Saving Running-Config to Startup Config 413
Schedule Refresh Monitor Targets 218
Schedules
Portlet 649
Scheduling 671
scheduling actions 90
Scheduling Monitor Target Refresh 218
Script Monitor Example 311
Search
In Portlets 449
Indexes 674
Search Indexes 382
Secure Connections 28
Secure connections, application and mediation servers 28
Secure WBEM Access 70
Self Management 185
Self Monitoring 185
Self-signed Certificate 714
SELINUX 415
Server 393
Monitor 27
Statistics 167
Server Information 414
Server log Maintenance 78
Service
Verification 197
Serving Multiple Customer Accounts 353
setting
time formats 82
Settings 445
Settings window 451
Show Performance Templates 232
Show Versions 672
showversions 382
Site Id Filtering 369
Site Management 358
Access Profiles 354
Editor 363
Portlet 354
Site Map portlet 652
SIteminder 44
SMTP 715
SMTP Mail Sender 418
SMTP, configuring 626
SNMP 383, 715
Interface Monitor 214
Interface Monitor Example 186
Monitor 212
Performance Monitoring Example 186
Table Monitor 215
Sorting 447
Spanning Tree Protocol (STP) 715
SSH (Secure Shell) 715
SSL 28, 29
SSL (Secure Sockets Layer) 715
SSL between application and mediation servers 28
Standalone Database Installation Problems 375
Standard Change Management Policies 339
Starting
Application server 77, 372
Web Client 28

Web Server 77, 372
Starting and Stopping Servers 378
Startup Failures 382
Startup Issues 375
Startup issues for Windows installations 377
Stopping
Application Server 77, 372
Web Server. 77, 372
Stopping LDAP Authentication 38
Sub-Policies 693
Supported
Flow versions 239
PowerConnect Models 67
Syslog Escalation Criteria 489
System Maintenance 76

T

Telnet 383
Tenant Reports 189
Terms of Use 31
Testing Remote WMI Connectivity 398
TFTP Servers 151
Threshold
Display 183
Graph Background 183
time format settings 82
time stamps 447
Timeout 386
tooltips 448
Top [Asset] Monitors Portlets 220
Top Configuration Backups Portlet 222
Top N Portlets
Calculations 220, 536
Topological correlation 219
Topology 516
Balloon 527
Circular 527
OVERVIEW 524
Radial 527
Saving 521
topology
layout 525
Topology Icon Size 516
topology labels, extending length 147
topology view
exporting to Visio 148
topology view, creating 147
trace 392
Traffic Flow
Device Limitations 239
Device Setup Examples 244
Drill Down 253
Performance Tuning 240
Search 254
Snapshot 255
Traffic Flow Database Advice 242
Trap (SNMP Trap) 715
Trap Forwarding 715
Trap Forwarding process 97
Triggering Bandwidth Calculations 217
Troubleshooting 371
Alarm 386
Alarm / Performance / Database 386
Backup/Restore 385
Common Problems 383
Create Process failed 374, 379
Database 386
Debug 392
Deploying firmware fails 385
Device O/S Overrides 385
Discovery 62, 384
Discovery Problems 383
Failures on Startup 378
File Problems 373
getlogs 394
Increasing Startup Logging 394
Installer Failure 373
Install-From Directory 375
JMX Console 414
Log Retention 394
Login Failures 379
Logs 394
logs.jar 394
My Alerts 444
MySQL Too Many Connections 391
Network Monitoring 387
Other Failures on Startup 378
Patches 391
Performance 386
Preventing Discovery Problems 383
Resolving Port Conflicts 393
showversions 382
Startup Failures 382
Timeout 386
Tips 77, 371
Unsynchronized Clocks in Clustered Installations 378
Upgrade / Data Migration Fails 382
Users and Organizations 382, 674
version.txt 382
Troubleshooting Adaptive CLI 317
Troubleshooting Flow 379
Tuning Log Retention 394
Turning on debugging 392

U

Uninstall 374
Unknown Traps 634
Unsynchronized Clocks in Clustered Installations 378
Update Location 512, 647
Updating Driver Patches 417
Updating Polling Subscriptions 219
Updating Your License 19
Upgrade / Data Migration Fails 382
Upgrade adds permissions 681
Upgrade Installations 417
Upgrading
  Licenses from previous version 19
User
  Login Report 135
  Role 675
  Screen Name length 71
User Site Access 366
User Site Access Policy 367
users
  creating 49
using containers 145

V

Vendors
  Portlet 641
  Snap Panel 644
Verify Administrator Credentials 398
version.txt 382
Versions 382
Visualization 516
Visualize
  Alarms 530
  As filter 517
  Balloon 527
  Circular 527
  Circular Layout 527
  Container display settings 509
  Global Settings 528
  Hierarchical-Cyclic 526
  Layout 525
  Layouts panel 525
  Legend Tab 528
  Links in Visualization 531
  My Network 516
  Node alarms 530
  Organic 527
  Overview 524
  Properties and Settings > Properties 528
  Radial 527
  Saving Views 521
  Tools 518
  Top-Level Nodes Tab 529
  View 521
  Views 522, 665
VLAN 715

W

WBEM 68
  Prerequisites 69
  root login 69, 408
  Web-Based Enterprise Management 68
Web client timeout override 688
Web Portal 389
Web Server 416
Web Server Property Overrides 71
Web Services ports 28, 698
Why share a schema? 272
Widgets panel 451
windows
  Settings 451
WMI 67, 383, 710
  ports 710
  Windows Management Instrumentation 67, 710
WMI and Operating Systems 396
WMI Authentication 402
WMI Troubleshooting 396
WMI Troubleshooting Procedures 395

X

XML Event Definition 115